DISSERTATION

ON

BREAKING THE DIGITAL CHAINS: A COMPREHENSIVE ANALYSIS OF CYBER FORENSICS AND LEGAL FRAMEWORKS FOR PROTECTING WOMEN ONLINE

LL.M. Dissertation submitted in the partial fulfilment of the requirements for the Degree of Master of Laws at the Sister Nivedita University, Kolkata

Submitted by:

MODHURIMA DALUI

Enrollment Number: 2222215005017
Registration Number: 220050175232
Session: 2022-2024

Under the Guidance of:

Mrs. SOMANJANA DUTTA CHATTAKHANDI
(Assistant Professor, School of Law)

Sister Nivedita University, Kolkata

Department of Law

Sister Nivedita University

2024

Sister Nivedita University
DG Block, 1/2 (Newtown), Action Area I, Kolkata – 7000156
Phone: +91 7595044470, 75950444709, 830653112
Official Website: https://snuniv.ac.in
Email: info@snuniv.ac.in

CERTIFICATE

This is to certify that the Dissertation titles **"Breaking the Digital Chains: A Comprehensive Analysis of Cyber Forensics and Legal Frameworks for Protecting Women Online",** has been submitted by **Miss. Modhurima Dalui,** bearing **Enrollment No: 2222215005017, Registration No: 220050175232** for partial fulfilments of the Degree of **Master of Laws (LL.M.)** from **Sister Nivedita University** under my guidance. It is his original work and may be placed before the examiners for evaluation.

This research work has not been submitted for the award of any other degree of this University or of any other University

Date: 25/4/25
Place: Kolkata

Mrs. Somanjana Dutta Chattakhandi
Assistant Professor of Law
School of Law (SNU)

DECLARATION BY THE STUDENT

I hereby declare that the work which is being presented in this dissertation "*Breaking the Digital Chains: A Comprehensive Analysis of Cyber Forensics and Legal Frameworks for protecting women online*" in partial fulfilment of the requirements for the award of the degree of Master of Laws in Criminal Law is an authentic record of my own work carried out during the period from 2022 to 2024 under the supervision of **Mrs. Somanjana Dutta Chattakhandi,**(Assistant Professor of Law) School of Law, Sister Nivedita University

I acknowledge that I have read and understood the UGC regulations, 2018 (*Promotion of Academic integrity and Prevention of Plagiarism in Higher Educational Institutions*).

I confirm that this dissertation has been checked for plagiarism using the plagiarism checking software Turnitin. At the end of the dissertation, a copy of the summary report demonstrating similarities in content and its potential source (if any), generated online using plagiarism checking software is enclosed. I herewith confirm that the dissertation has been less than 10% similarity according to the plagiarism checking software's report and meets the UGC Regulations as well as plagiarism rules of Sister Nivedita University.

I further declare that no portion of the dissertation or its data will be published without the Institute's or supervisor's permission. I have not previously applied for any other degree or award using the topics and findings described in my dissertations.

Name of the Student: **Modhurima Dalui**

Registration No.: **220050175232**

Department: **School of Law**

PREFACE

In the digital age, the promise of connectivity and empowerment has also brought with it a disturbing rise in cyber threats, particularly targeting women. From online harassment and image-based abuse to cyber-stalking, doxxing, and the increasingly prevalent deep fake crimes, the virtual world has become an extension of the violence and discrimination that women often face offline. These digital forms of abuse are not only invasive but often traumatic, inflicting psychological, emotional, reputational, and sometimes even physical harm. Perpetrators exploit the anonymity and borderless nature of the internet, making it increasingly difficult for victims to seek justice and protection within conventional legal systems.

This ever-evolving digital age, the complexity and frequency of cybercrimes demand a holistic and multi-disciplinary approach to prevention, investigation, and justice. As our lives become increasingly intertwined with digital platforms, the nature of crime has also shifted—transcending geographical boundaries, exploiting technological loopholes, and often leaving behind minimal physical traces. In this context, cyber forensics has emerged as a pivotal branch of forensic science, playing a crucial role in identifying, preserving, analyzing, and presenting digital evidence in a legally admissible manner. Whether it's tracing the origins of malicious cyber-attacks, unmasking anonymous perpetrators, retrieving deleted data, or authenticating digital content, cyber forensics provides law enforcement agencies and judicial authorities with the technical means to pursue justice in the virtual realm.

The urgent need to address these multifaceted challenges forms the foundation of this work. As technology evolves, so too must our understanding of how it intersects with gender-based violence. This calls for a holistic approach that combines legal reform, technological advancement, social awareness, and institutional accountability. There is a pressing necessity to strengthen cyber forensic capabilities for effective investigation and prosecution of digital crimes, while simultaneously evolving legal frameworks to reflect the complexities of the digital landscape Therefore, this research focuses to study the various types of cybercrimes rising against women and analyses the rising trends of these crimes against women in India. It also aims to critically examine the intersection of cyber forensics, digital rights, and the evolving legal landscape with a gender-sensitive lens. This study delves into the role of cyber forensics in tracing digital crimes, the importance of digital evidence in prosecution, and the comparative effectiveness of legal frameworks in India and globally—especially in the UK, USA, and Canada.

The objective of this research is not only to highlight the gaps in existing laws and investigative mechanisms but also to advocate for a more robust, inclusive, and technologically adaptive legal structure. By identifying loopholes, examining case studies, and suggesting strategic reforms. Thus this study aims to critically explore the role of cyber forensics and assess the effectiveness of current legal frameworks, while advocating for a more gender-sensitive, technologically adapt, and victim-centric approach in protecting women online.

It is is dedicated to all the women whose voices have been silenced in cyberspace—and to the on-going global efforts to ensure that the internet becomes a safer, more equitable space for everyone.

ACKNOWLEDGEMENT

I express my deepest gratitude to **Mrs. SOMANJANA DUTTA CHATTAKHANDI, Assistant Professor of Law, School of Law, Sister Nivedita** University, New Town, Kolkata, whose unwavering support, insightful guidance, and constant encouragement have been instrumental in shaping the course of this research. Despite her numerous responsibilities, she graciously devoted her time and attention to my work, offering invaluable suggestions and fostering my academic growth throughout the research journey.

I extend my heartfelt thanks to the **entire faculty of the School of Law, Sister Nivedita University**, for their continuous support, intellectual inputs, and generosity in providing their time and insisghts, all of which greatly enriched the quality and depth of this research.

I owe a special debt of gratitude to my **family and friends** for their unwavering emotional support constant inspiration, and steadfast belief in my capabilities. Their encouragement served as a pillar of strength during moments of doubt and difficulty.

Above all, I am eternally thankful to **God**, my source of wisdom and strength, for blessing me the intellect, motivation, passion, and resilience to pursue and complete this work with dedication and purpose.

Finally, I extend my sincere appreciation to **all those who, in one way or another, contributed to the successful completion of this dissertation.** Your support has been deeply valued and sincerely acknowledged.

Place: Kolkata

Date: 25.4.25

Modhurima Dalui

Modhurima Dalui

LIST OF ABBREVIATIONS

PTSD: Post-Traumatic Stress Disorder

WWW: World Wide Web

IOT: Internet of Things

SMS: Short Message Service

MMS: Multimedia Messaging Service

SD: Secure Digital

SSD: Solid State Drive

CD: Compact Disc

DVD: Digital Versatile Disc or Digital Video Disc

GPS: Global Positioning System

USB: Universal Serial Bus

CRC: Cyclic Redundancy Check

MD5: Message Digest Algorithm 5

PDF: Portable Document Format

ZIP: Zigzag Inline Package

IC3: Internet Crime Complaint Centre

CMS: Content Management System

DNA: Deoxyribonucleic Acid

NCA: National Crime Agency

GREVIO: Group of Experts Action against Violence against Women and Domestic Violence

NGO: Non-Governmental Organization

UNCITRAL: United Nations Commission on International Trade Law

UK: United Kingdom

USA: United States of America

FBI: Federal Bureau of Investigation

AIR: All India Report

NCRB: National Crime Records Bureau

NCW: National Commission for Women

IT: Information Technology

IPC: Indian Penal Code

BSA: Bhartiya Shakshya Adhiniyam

BNS: Bhartiya Nyaya Sanhita

LIST OF CASES

Page No:

Anvar P.V. v. P.K. Basheer & Ors (2014 10 SCC 473----------32

Suhas Katti v. State of Tamil Nadu (CC. No. 4680 of 2004)---------- 33

Shafhi Mohammad v. State of Himachal Pradesh, SLP(Crl.)No.2302 of 2017----------33

United States v Yung, 37 (3d Cir 2020)----------52

United States v Sayer, 748 (1st Cir 2014)----------52

United States v Moreira, 5 F Supp 3d 1290 (SD Fla 2014)----------53

Doe v Google LLC (2021) (ND Cal)----------55

Patterson v. California (2018) (ND Cal)----------55

Commonwealth v. Markoff, No. SUCR2009-10614 (Mass. Sup. Ct. 2009)----------64

Grant v. Southwestern and County Properties Ltd (Mass. Sup. Ct. 2015)----------65

R v Ghomeshi [2016] ONSC 7671----------65

R. *v.* Jarvis, 2019 SCC 10, [2019] 1 S.C.R. 488----------66

Manish Kathuria vs. Ritu Kohli AIR 2001----------75

State Cyber Cell vs. Yogesh Pandurang Prabhu, CC No. 686/PS/2009----------75

Avinash Bajaj vs. State (N.C.T) of Delhi AIR 2004----------76

State of Tamil Nadu v. Dr. L. Prakash, writ petition no. 7313 of 2002----------76

Tamal Chakraborty v. State of West Bengal AIR 2019----------76

Fatima Riswana v. State Rep. by ACP., Chennai & Ors AIR 2005 712----------77

Aarti Tiwari v. State of Chandigarh, MANU/CG/0285/2014----------78

State v. Jawant Kumar Das, Manu /TN/0676/2002----------77

Shreya Singhal vs. Union of India, CC 167 of 2012----------77

State vs. Ts. Balan and Aneesh Balan, B.A. NO.799 0F 2016----------78

Sreekanth C.Nair vs Licensee/Developer (2008)----------79

Kirti Vashisht v. State of Delhi 2019 SCC Online Del 11713----------79

Sree Surya v. State of Kerala, Kerala High Court Case No. 2022----------79

Kalindi Charan Lenka v. State of Odisha Crl. Appeal No. 157 of 2018----------79

Kamlesh Vaswani v. Union of India AIR 2016----------80

Sabu Mathew v. Union of India AIR 2008----------80

Neha Ghai case----------80

Salem case----------80

Prajwala v. Union of India air 2015----------81

TABLE OF CONTENTS

Page No:

CERTIFICATE----------i

SELF DECLARATION----------ii

PREFACE----------iii

ACKNOWLEDGEMENT----------iv

LIST OF ABBREVIATIONS----------v

LIST OF CASES---------- vi

CHAPTER: 1----------1-10

1. INTRODUCTION

1.1.Introduction----------1

1.2.Research Problem----------3

1.3.Scope and Relevance of the Study----------3

1.4.Research Objectives----------4

1.5.Research Questions----------4

1.6.Hypothesis----------4

1.7.Research Methodology----------4

1.8.Literature Review----------5

1.9.Framework of the Study----------10

CHAPTER: 2----------11-27

2. CYBERCRIME AGAINST WOMEN IN INDIA: A MENANCE OF VIRTUAL VIOLENCE

2.1.Introduction----------11

2.1.1.Reported cybercrime against women in India----------12

2.1.2.State-wise analysis of the highest reported cybercrimes against women----------14

2.2.Types of Cybercrime against women----------15

2.2.1.Cyber Defamation----------16

2.2.2.Cyber Stalking----------18

2.2.3.Cyber Blackmailing----------20

2.2.4.Cyber Pornography----------22

2.3.Data Analysis----------24

2.3.1.Sample Design----------24

2.3.2.Detailed Analysis of the Responses----------25

CHAPTER:3----------28-48

3. **CYBER FORENSICS IN THE ERA OF DIGITAL TRANSFORMATION: ASSESSING ITS ROLE IN INVESTIGATING CYBER-CRIME AGAINST WOMEN**

3.1 What is Cyber Forensic----------29

3.2 Classification of Cyber Forensic---------- 30

3.2.1. Network Forensic----------30

3.2.2. Mobile-device Forensic----------31

3.2.3. Computer Forensic----------31

3.2.4. Malware Forensic----------31

3.2.5. Cloud Forensic----------31

3.2.6. Social Media Forensic----------31

3.2.7. IOT Forensic----------31

3.3. The Nexus of Cyber Forensic and Digital Evidence----------32

3.4. Tools and Techniques used for Investigating Cybercrimes against Women----------35

3.4.1. Forensic Tools used for Data Recovery----------36

3.4.2. Forensic Tools used for Mobile Devices----------37

3.4.3. Forensic Tools used for Password Recovery----------38

3.4.4. Forensic Tools used for Network Analysis----------38

3.4.5. Forensic Tools used for Obscene Content Takedown----------39

3.4.6. Forensic Tools used for Social Media monitoring----------40

3.5 Advantages of Cyber Forensics----------41

3.6. Challenges Of Cyber Forensics----------41
3.7. Data Analysis----------43
3.7.1. Sample Design :----------43
3.7.2. Detailed Analysis----------44
CHAPTER: 4----------49-66
4. CROSSING JURISDICTIONAL LINES:A COMPARATIVE LEGAL STUDY ON CYBERCRIME AGAINST WOMEN IN UK, USA, CANADA
4.1. Introduction----------49
4.2. Cyber Crime Against Women in USA----------51
4.3. Cyber Crime Against Women in UK----------55
4.4. Cyber Crime Against Women in CANADA----------59
4.5. International Conventions for Cybercrime Against Women----------61
4.5.1. The Istanbul Convention----------62
4.5.2. The Budapest Convention----------63
4.6. Admissibility of Digital Evidence----------64
CHAPTER: 5----------67-84
5. SAFEGUARDING WOMEN: THE JUDICIARY'S ROLE IN COMBATTING CYBER CRIME AGAINST WOMEN IN INDIA
5.1. Legal Frameworks Protecting Women----------68
5.2. Landmark Judgements----------74
5.3. Challenges in Addressing Cyber Crimes Against Women----------82
CHAPTER 6:----------85-87
6. CONCLUSION----------85

BIBLIOGRAPHY----------A

CHAPTER:- 1

INTRODUCTION

1.1 Introduction

"Technology is a useful servant but a dangerous master, and the internet is no exception."

– Christian Louis Lange[1]

The continuous development of technology has drastically changed how individuals interact, collaborate, and navigate their daily lives. The rapid growth of technology has transformed the digital landscape, offering unprecedented opportunities for communication, information exchange, and social engagement. However, this progress has also given rise to new types of cybercrimes and has become a global threat. The last decade has witnessed a substantial rise in internet usage. About 2.77 billion individuals, or roughly 38% of the world's population, were internet users in 2014 alone. This figure has increased to 5.52 billion users by 2024, representing 67.5% of the world's population, meaning a 99% growth of internet users during a ten-year period.[2] Online platforms especially social media has seen a substantial rise in users alongside overall internet growth. More than 60% of internet users are active on social media.[3] While the internet is a blessing that connects us like never before, it also isolates us within our digital echo chambers. In this digital age, almost every individual has encountered the consequences of online interactions, whether in the form of cyber threats, privacy breaches, or social media influences. However, women remain particularly vulnerable, facing a higher risk of cyber harassment, online exploitation, and digital abuse.[4] Cybercrime is the term used to describe actions that are performed to injure a person using an electronic device or the internet. The word 'cybercrime' was coined in 1982 by William Gibson. Cybercrime is a relatively new phenomenon that has emerged with the progression of new technologies. The Oxford Dictionary states, 'Cybercrimes are those criminal activities carried out using

[1] Christian Louis Lange, Norwegian Peace Advocate, Historian and Political Scientist (1869 – 1938)

[2] Statista, *'Internet usage worldwide – statistics & facts'* < https://www.statista.com/topics/1145/internet-usage-worldwide/#topicOverview> accessed 15th January, 2025

[3] Ibid.

[4] S. R. Balabantaray, M. Mishra, U. Pani, *'A Sociological Study of Cybercrimes Against Women in India: Deciphering the causes and evaluating the Impact on the Victims'* (2023) 19 IJAPS 25

computers or the internet'. These crimes are the by-product of new technological innovations where technically skilled criminals target people to cause harm.[5]

From the ancient times, Indian women are regarded as goddesses in cultural and religious traditions but still they experience numerous sorts of violence. Ironically, in a country that upholds the worship of women, they are also the most frequent victims of crimes such as rape, molestation, domestic abuse, acid attacks, and different forms of gender-based violence.[6] Women are not exempt in the digital sphere due to the internet's explosive expansion. A global problem, the emergence of cyber violence against women and girls adds a digital element to gender-based violence with potentially serious physical, sexual, and psychological repercussions.[7] The United Nations reports that women are the recipients of approximately 95% of all online hostility, including harassment, offensive language, and defamatory content.[8] Cyber-crime and victimisation of women in the digital space has turned to be an alarming issue, from internet trolls to deep fakes gender-based violence in the online world is a pressing concern that demands urgent attention. There has been a strong association between cyber violence and an increased risk of suicidal behaviour. Victims of online harassment, cyber bullying, and other forms of digital abuse often experience heightened levels of depression and anxiety, which can lead to suicidal thoughts and actions.[9] Among the countries, India is one of the very few to have enacted the "Information Technology Act, 2000", to combat cybercrimes. However, the Act still falls short in adequately addressing issues specifically related to women. It is important to recognize how the use of contemporary information and communication technology has allowed crimes like rape, molestation, blackmail, and stalking to adapt to the digital age. Incidents now include recording rape scenes on mobile devices, blackmailing women with intimate images, grooming for online porn markets, and the sexual exploitation of teenage girls by showing them explicit content via phones or computers. Additionally, women are frequently harassed through persistent calls, SMS, MMS, and instant messaging on digital platforms.[10] It has been

[5] O.Goni, H.Ali, *The Basic Concept of Cybercrime (2022),* 1(2) JTIE 16
[6] Upasana Borah*, 'Cyber Crime Against Women in the Digital Era: A brief Indian Scenario'* 8 IJRASET 615
[7] EIGE, European Union, *'Combating Cyber Violence against Women and Girls.pdf'(2022)*
[8] Isabel Santagostino Recavarren, *'Protecting Women and girls from cyber harassment: a global assessment'* (2023) <https://blogs.worldbank.org/en/developmenttalk/protecting-women-and-girls-cyber-harassment-global-assessment> accessed 15th January, 2025
[9] Zhiwei Lu, *'Concern on cyber violence and suicide during Covid-19 pandemic'* (2022) < ttps://www.frontiersin.org/journals/psychiatry/articles/10.3389/fpsyt.2022.956328> accessed 16th January, 2025
[10] Debarati Halder, K. Jaishankar, '*Cyber Crimes against women in India'* (Sage Publication, 2017)

observed that, in addition to the high number of reported cybercrimes against women, many incidents go unreported as women often refrain from filing complaints due to social stigma and family pressures.

1.2 Research Problem:

Globally, cybercrime against women is becoming more common, which has led to major worries about digital safety, privacy, and justice. Online gender-based violence has increased due to the growth of digital platforms, especially in India. The number of cybercrimes targeting women has significantly increased in the nation throughout the last five years. Even though the development of the field of cyber forensics has helped to some degree to combat online crimes against women, the implementation of current legislative frameworks is still insufficient to adequately handle cyber threats that are specific to gender. This study looks at how cyber-forensics can be used to combat these kinds of crimes. It also assesses legal interventions to find weaknesses and suggest changes that will improve victim protection and law enforcement effectiveness. This study conducts a comparative analysis to investigate possible reforms for a stronger cyber-justice system in India.

1.3 Scope and Relevance of the Study:

- This research will look at the growing number of cybercrimes against women in India, concentrating on finding trends in the growth and investigating recently discovered online offenses that target women
- This research intends to investigate the critical role that cyber forensics plays in preventing cybercrimes against women in India by examining the methods and instruments used in investigations and assessing how well cyber forensics manages digital evidence
- This research aims to investigate the admissibility of digital evidence in foreign courts and will compare the UK, USA, and Canada in order to assess various legal reforms and case studies in the fight against digital offenses against women
- This research will assess India's current cybercrime laws and regulations to prevent digital crimes against women and identify any legal loopholes that require urgent correction to address women's online vulnerabilities

- This research will also examine the causes and issues of the increased prevalence of cybercrime against women online, as well as the difficulties in preventing such crimes.

1.4 Research Objectives:

The primary and secondary objectives of the research on cyber-crime against women in India are as follows:

1) To analyse the different types of cybercrime up surging against women in India and identifying the growth patterns

2) To uphold the vital role of cyber forensics in curbing the various types of cyber-crimes against women.

3) To analyse the implementation of the judiciary and legal frameworks in combatting cyber-crimes against women

1.5 Research Questions:

1) How far cyber-forensics helps in the investigation and in controlling cyber-crimes against women in India?

2) What is the role of the judiciary and it's contribution in combating cybercrime against women in India?

1.6 Hypothesis:

Due to lack of proper legislative measures and challenges faced by the judicial system, there has been a significant rise of cybercrime against women in India.

1.7 Research Methodology:

The research has been conducted using both doctrinal and empirical research. This research paper is based on both primary and secondary data like internet surveys, field study, crime reports, case reports, journals etc. The empirical study of this research has been conducted by Non-Probability Sampling method where the samples are collected by using Purposive Sampling method and Convenience Sampling Method. Therefore, a total of 80 samples were collected (n-80) to conduct this research out of which 30 samples includes experts in the cyber-forensic fields such as cyber forensic experts and cyber-crime investigators and 50 samples includes cyber-crime victims and women from different age groups.

1.8 Literature Review:

1. In the book ***'Cyber Crimes against Women in India'***, by **Dr. Debarati Halder and K. Jaishankar**, by "Sage publications", they have beautifully discussed about the various types of cyber-crimes against women. They have also outlined that why women are victimized online and have also discussed the procedural practices for investigation, prosecution, arrest and detention. They have also discussed about the various legal frameworks to combat such crimes. However, they have failed to deliver the recent up gradations and motives behind the different types of cyber-crimes against women and also have not discussed the role of digital evidence in these cases.
2. In another book named ***'Cybercrime and the Victimization of Women: Laws Rights and Regulations'*** by **Dr. Debarati Halder and K. Jaishankar** by "Sage Publications", they have beautifully outlined various case studies and also different regulations controlling cyber-crime against women. However, they have analysed in details about the legal frameworks of different countries. Yet, they have failed to deliver the recent up gradations and motives behind the different types of cyber-crimes against women and also have not discussed the role of digital evidence in these cases.
3. In the book ***'Cyber Forensics'*** by **Mr. Dejey Murugan**, of the "Oxford Publication", has beautifully outline the core concepts of digital forensics, it's processes, tools and also the cyber laws pertaining to both Indian and International Context with interesting case studies. It has also beautifully discussed the analysis, acquisition and admissibility of Digital Evidence. However, it has not covered the forensics role in combatting different online crimes and has not discussed it's practical applicability in handling such crimes.
4. In the book ***'Cyber Crimes Against Women: An Indian Law Perspective'*** by **Dr. Karnika Seth** of "Oxford Publication" has discussed the different types of cyber-crimes against women and cyber-crimes against girl child and has also discussed the laws in combatting such crimes. This book has also discussed the judiciary's role by discussing through various case laws in combating such crimes against women. However, there has been no comparative analysis of the legal frameworks across different countries in addressing and controlling such crimes.
5. In the book ***'Cyber crime against women in India'*** by **Dr. Sashya Mishra** by "Notion Press", has elaboratively discusses the growth trends of cyber-crimes against

women. It has also discussed how women are victimized through different social media platforms. It has also discussed the rising concerns and the motives that why women fall prey to cyber-crimes. However, it has not covered the legal perspective and the laws to combat such crimes.

6. In the book ***'Digital Forensics and Investigation Methods'*** **by Dr. Padmavathi Ganapathi and Dr. Digvijay Singh** by "Notion Press" has outlined the important role of digital forensics and it's investigation methods. It explains about different digital forensic investigation models and the process involved in digital forensic analysis. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crimes pertaining to women.
7. In the article ***'A Sociological Study of Cybercrimes against women in India: Deciphering the causes and evaluating the impact on the victims'*** **by Subhra Rajat Balabantaray and Mausami Mishra** of the "International Journal of Asia-Pacific Studies (IJAPS)", it has discussed about the rising trends of cyber-crimes against women over the past years and has outlined the prime causes of these crimes. This article has also discussed the social consequences of cybercrimes on women and girls. However, the legal perspective has been kept untouched in this article.
8. In the article ***'Cyber Crime against Women in the Digital Era: A Brief Indian Scenario'*** **by Upasana Borah** of the "International Journal for Research in Applied Science and Technology (IJRASET)", it has discussed about the legal frameworks that aim to control these crimes against women. This paper has also brought forward the historical background and the sociological reasons of cyber-crime against women. However, there has been limited research on the judiciary's role in controlling such crimes in India.
9. In the article ***'Cyber crime against women increasing threat to security of Indian Women'*** **by Dr. J.D. Lekurwale** of the "International Research Journal of Management Sociology and Humanities (IRJMSH)" has elboratively discussed the concept of cyber-crime against women and it's causes. This paper has also highlighted various states in India that reports an increased cases of cyber-crimes against women. However, the legal perspective has been kept untouched in this article.
10. In the article, ***'Cyber crimes against women in India'*** **by Dr. T. Sadashivam** of "International Journal of Ideas (IJI)" has discussed the rising trends of cybercrimes against women highlighting the most vulnerable states. This article has also discussed

the legal frameworks that protects women online and has also highlighted various case laws. However, there has been limited research on the judiciary's role in controlling such crimes in India.

11. In the article, ***'The Increasing trends of Cyber Crimes Against Women: An Indian Perspective'*** **by Dr. G. Mallikarjun** of the "Journal of Emerging Technologies and Innovative Research (JETIR)" has made a detailed analysis of the different types of cyber-crimes against women in India. It has also discussed the various laws protecting women online and has also highlighted various case laws and the judiciary's role in protecting women online. However, a comparative analysis of the legal frameworks across different countries would have brought forward the significant role of the Indian laws.
12. In the article, ***'Victimization of Women Beneath Cyberspace in Indian Upbringing'*** **by Dr. Monika Jain** of "Bharti Law Review (BLR)" has offered an overview and analysis of the development of regulatory instruments, such as statutes, recommendations, guidelines, and other measures, aimed at safeguarding the privacy and related interests of women in cyberspace. The paper also provides a predictive analysis of cybercrimes targeting women in India, along with the examination of laws to prevent cyber victimization of women. However, a comparative analysis of the legal frameworks across different countries would have brought forward the significant role of the Indian laws.
13. In the article, ***'Cyber Crime against women in Indian Context: An Overview'*** **by Priya Gupta** of the "Journal of Research in Humanities and Social Science (JRHSS)" has beautifully discussed the various legal frameworks and judicial pronouncements to control cyber-crime against women. However, the article has failed to discuss the different types of cyber-crimes against women and has not discussed the reasons affecting it.
14. In the article, ***'An Historical Perspective of Digital Evidence: A forensic scientist's view'*** **by Carrie Morgan Whitcomb,** of "International Journal of Digital Evidence (IJDE") has elaboratively highlighted the historical background of digital evidence and has discussed the accreditation and certification of Digital Evidences. The article though has discussed the major role of digital evidence, yet it has failed to discuss the role digital evidence in different types of cyber related cases.
15. In the article, ***'Obscenity and the Depiction of Women in Pornography'*** **by Siddharth S. Aatreya** of the "Nalsar Student Law Review (NSLR)" has beautifully

depicted that how women fall victims of cyber pornography it's legal consequences and also also described the role of judiciary by elaboratively discussing about various case laws. This article has also highlighted various case laws from UK and the USA. However, there has been no comparative analysis of the legal provisisons of other countries.

16. In the article, ***'Digital victimization of Women in Cyberspace'*** **by Ms. Akansha Pathak and Mr. Prateek Tripathi** of the "National Law University Assam Law Review (NLUALR)" has beautifully described the different types of cyber-crimes against women and the reasons that causes women to fall victims of these crimes in the cyber space. It has also discussed various legal frameworks to control such crimes. However, a comparative analysis of the legal frameworks across different countries would have brought forward the significant role of the Indian laws.
17. In the article, ***'Adjudication Processes of Cyber Offenses & Cyber Crimes with Womans in India'*** **by Gourav Kumar Shaw,** of "International Journal of Public Policy (IJPP)" has discussed about cybercrime and it's types against women. It has also discussed the legal frameworks and the judiciary's approach in protecting women online. However, there has been no comparative analysis of the legal frameworks across different countries in addressing and controlling such crimes.
18. In the article, ***'Cyber Crime Against Women: Right to Privacy and Other Issues'*** **by Sanjeev Kumar and Priyanka** of "Journal of Legal Studies and Research (JLSR)" has discussed the types of cyber-crimes against women and has highlighted the reasons for the growth of cyber-crime against women in India by highlighting the legal and sociological reasons. This article has also put light on the legal frameworks and the constitutional liability of cyber crimes against women. However, there has been no comparative analysis of the legal frameworks across different countries in addressing and controlling such crimes.
19. In the article, ***'Cybercrime and Digital Forensics: Technologies and Approaches'*** **by Cisar P. Maravic** of the "DAAM International Scientific Book (Ch.42)" has discussed and explained the concept of 'cybercrime,' outlining its various categories and the structure of different types of attacks, which are the primary forms of cybercrime. It has also focused on digital forensics, which is the core procedure for investigating digital crime scenes. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crime against women.

20. In the article, ***' Cyber Forensic – A Literature Review'*** **by Aparna Chaturvedi,** of the "Trinity Journal of Managemnt, IT and Media (TJMIM)" has brought forward the branch of cyber forensic in cyber crime investigation and has discussed it's tools and techniques in dealing with such crimes. It has also highlighted the various branches of cyber forensics and has outlines it's policies and procedures. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crime against women.

21. In the article, ***'The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection'*** **by Jaydevsinh B. Vala** of "International Journal of Life Sciences, Biotechnology and Pharma Research (IJLSBPR)" has discussed about the need of Digital Forensic in Cyber Crime Detection and has also discussed the various branches of cyber forensics in investigation cyber crimes. The paper has also discussed the important role of digital evidence and the process and procedures in extracting such evidences. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crime against women.

22. In the article, ***'Digital Forensic Tools Used in Analysing Cybercrime'*** **by Mohammad Dweikat**, of "Journal of University of Shanghai for science and technology (JUSST)" has outlined the investigation methods and models used to investigate cyber-crimes. It has also made a detailed analysis about the various branches of cyber-forensics used to deals with cybercrimes. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crime against women.

23. In the article, ***'Digital Forensics'*** **by Suwarna Nimkarde, Shobhana Gaikwad,** of the "International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)" has beautifully discussed the various branches of cyber forensics and how it plays an important role in the criminal justice system and how the evidences are taken from cyber related cases. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crime against women and how the evidences are used in cyber cases related to women.

24. In the article, ***'Role of Cyber Forensics in Investigation of Cyber Crimes'*** **by Prashant Saurabh and Amrit Jay Kumar Roy** of the "International Journal of Law Management and Humanities (IJLMH)" has beautifully described the role of cyber forensic in controlling cyber-crime and also describes the various branches of cyber forensics in dealing with cyber-crimes. However, it has not outlined that how the

digital forensic branch helps in controlling cyber-crime against women and how the evidences are used in cyber cases related to women.

25. In the article, ***'Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings'*** **by Rahul K. Bharati and Dr. Shobha K. Bawiskar** of the "International Journal of Scientific Research in Science and Technology (IJSRST)" has discussed about how the digital evidences are accepted in legal proceedings and how the branch of cyber-forensics helps in the admissibility of digital evidence. It also discusses the challenges related to it. However, it has not outlined that how the digital forensic branch helps in controlling cyber-crime against women and how the evidences are used in cyber cases related to women.

1.9 Framework Of The Study

1. **CHAPTER: I –** INTRODUCTION

2. **CHAPTER**: **II** - CYBERCRIME AGAINST WOMEN IN INDIA: A MENACE OF VIRTUAL VIOLENCE.

3. **CHAPTER**: **III** – CYBER FORENSICS IN THE ERA OF DIGITAL TRANSFORMATION: ASSESSING IT'S ROLE IN INVESTIGATING CYBER CRIMES AGAINST WOMEN

4. **CHAPTER: IV –** CROSSING JURISDICTIONAL LINES: A COMPARATIVE LEGAL STUDY ON CYBER CRIME AGAINST WOMEN IN THE UK, USA, CANADA.

5. **CHAPTER: V** - SAFEGUARDING WOMEN: ASSESSING THE JUDICIARY'S ROLE IN COMBATTING CYBER CRIME AGAINST WOMEN IN INDIA.

6. **CHAPTER: VI** - CONCLUSION

CHAPTER: 2

CYBERCRIME AGAINST WOMEN IN INDIA: A MENACE OF VIRTUAL VIOLENCE

2.1 Introduction

The internet's explosive growth has increased the number of online crimes, making the environment risky for crimes based on gender. Women are evolving as vulnerable targets of these ever-expanding cybercrimes. Crime against women has long been a problem in society, and as digitalization has progressed, these crimes have expanded beyond physical injury; women are increasingly becoming victims of online wrongdoing. The digital landscape in India has seen a dramatic transformation in recent years, and the use of the internet has grown exponentially. According to the India Internet Report, in 2023, there has been a 27% surge in female internet users as compared to men, with only 18%. [11]This accessibility of the internet serves as a double-edged sword where women get immeasurable benefits, yet they face shocking consequences. This digital surge has created a paradox for women. Though they have benefited in many ways and have gained access to education, communication, and economic opportunities through the internet yet, despite the undeniable benefits, there has been an upsurge in cybercrime targeting women, where women become victims of online sexual exploitation, stalking, blackmailing, etc. The vast potential of the World Wide Web is continually mistreated by perpetrators as they use its speed and reach to circulate obscene materials easily within a short period. In today's world, one out of every ten women becomes a victim of cybercrime or confronts exploitation in cyberspace, among which women between the age group of 18 to 24 are seen to be the most vulnerable ones. It is mostly found that these criminals are the victims' relatives, lovers, and ex-partners.[12] Online platforms such as social media are commonly exploited by these cybercriminals, who try to fulfill their undesired pleasures by blackmailing, harassing, and exploiting women by sending obscene videos, stalking, and also developing pornographic images. Women often become victims of these crimes as they tend to share their private information out of trust, which is further

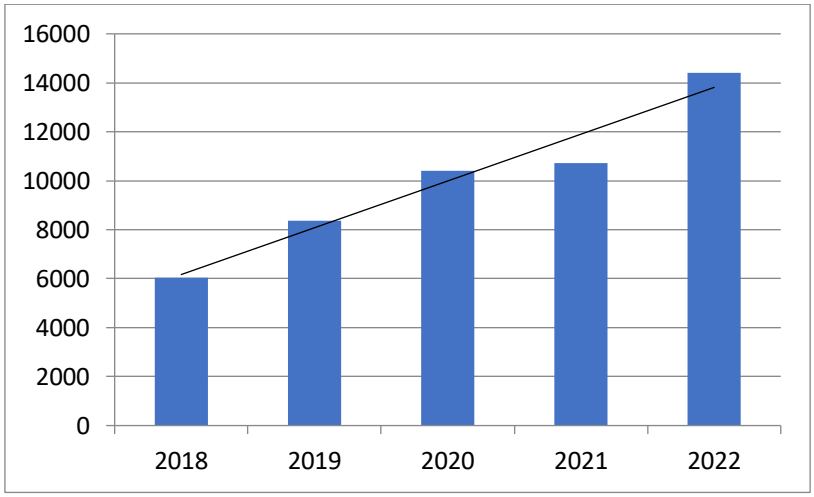
[11] Government of India, *Ministry of External Affairs, India Internet Report Dec'2022* < https://indbiz.gov.in/> accessed 20th March,2024

[12] European Institute for Gender Equality (EIGE), '*Combating Cyber Violence Against Women and Girls'* (EIGE 2022) [10-13] < https://eige.europa.eu/> accessed 20 March 2024

weaponized against them by the perpetrators.[13] These crimes can have a devastating impact on a woman's sense of self where a woman goes through social humiliation, psychological trauma, self-harm, economic loss, and various other consequences. However, women frequently hesitate to file accusations out of fear of social shame and disgrace, and many crimes go undetected because of ignorance. This low reporting rate allows cybercrimes to go unnoticed, creating a perception of women as easier targets for criminals. Apart from these issues, gender bias, discrimination, and anonymity over the internet are also the main factors contributing to women becoming victims of cybercrimes.[14]

Protecting women has always been a major concern of the penal law of the state, and with the evolution of crime, it is essential to extend its framework in cyberspace, where new threats and forms of harassment have emerged. According to the NCRB data i.e. the National Crime Records Bureau, there has been a significant rise of 24% in cybercrime against women in 2020, but it became even more alarming with a 34% rise in these crimes in 2022. However, since 2017 there has been a continuous rise of these crimes posing a concerning threat to society. The following Chart 1.1 outlines the increased rate of crimes that are reported against women in India from (2018-2022). However, many more cybercrimes against women likely go unreported than what appears in the reports and statistics.[15]

2.1.1 Reported cybercrime against women in India



Source: National Crime Records Bureau (NCRB) 2018 - 2022

[13] S.Kumar, Priyanka, '*Cyber Crime Against Women: Right to Privacy and other issues'* (2019) 5(5) JLSR <https://www.researchgate.net/publication/344153821>accessed 20 March 2024
[14] Government of India G20 Summit, *'Cyber Crime Against Women Summit'23'* (2023)
[15] NCRB Report, *Crime In India* Vol.2

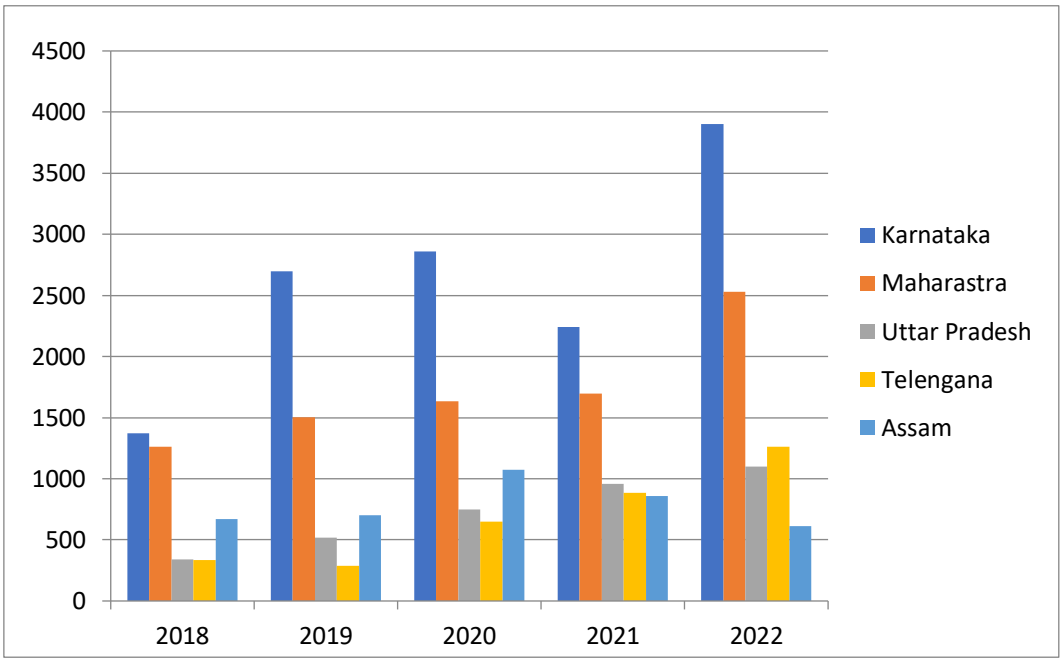
The chairperson of the NCW stated that among all the cybercrimes that are committed, 98% of them are committed against women.[9] Thus, the illegal actions committed by an individual or group of individuals to injure a woman emotionally and psychologically via the use of computers and the internet can be referred to as cybercrime against women. Today, the internet can alter voices images, and other elements potentially leading to severe social disorders. This misuse of the internet is frequently targeted against women by the perpetrators to fulfil their desires and through these illegal activities violate a woman's basic human right[16]. The "right to freedom of speech and expression" which is outlined in 'Article 19(1)(a)' has been expanded by the court over time. While the fundamental "right of speech and expression" is a basic right guaranteed to the citizens of India, and the use of the internet has advanced the reach of this fundamental right to millions of people, it has exposed women to a persistent cycle of cyber bullying, defamation, blackmailing, etc. Hence, this misuse of the right by the miscreants undermines its intended purpose. There is a close nexus between the fundamental "right to privacy" and the presentation of information in the cyber world, but this basic "right to privacy", which is a part of the "right to life" under 'Article 21' of the Indian Constitution, is infringed upon when a woman's personal information and obscene images get displayed in cyberspace.[17] The rate of cybercrime against women has been increasing as it includes several factors, such as emotional outrage, personal revenge, anger, dishonour, etc., that trigger criminals to commit such crimes. According to studies, increased use of mobile phones and the internet has exposed women and girls more to miscreants.[18] Women and girls experience harassment and stalking not only when they are connected to the internet or the 'World Wide Web'(WWW) but also through unnecessary phone calls and SMSs. Thus, these offenses are committed using all forms of electronic media and are not restricted to the use of the Internet only.[19]

Cybercrime against women has been a significant challenge all over India, but certain regions experience a higher amount of crime as compared to others. India has seen a significant rise in the internet penetration rate, jumping from 48.1% to 51.5% in 2023, which reflects a rise in active web users.[20] Notably, in 2023, gender-based active internet users were at 54% in cases

[16] Debarati Halder, K. Jaishankar, '*Cyber Crimes against women in India'* (Sage Publication, 2017)
[17] Shashya Mishra, '*Dimensions of Cybercrime Against Women in India – An Overview' (2018)*, 5 IJRAR 966
[18] Pallavi Singh, *Chapter 1: 'Introduction'* in '*Cyber Crime Against Women in India'* (PhD thesis, Banaras Hindu University, 2018) <https://shodhganga.inflibnet.ac.in/> accessed 20 March 2024
[19] Supra Note 7
[20] Global Digital Report, *'Digital 2023 : India'* < https://datareportal.com/reports/digital-2023-india> accessed 20th March,2024

of males and 46% in cases of females.[21] Regions with patriarchal attitudes and high internet penetration often see a rise in these crimes. States like Karnataka, Maharashtra, and Uttar Pradesh have consistently experienced a higher rate of cyber-crimes against women, followed by Assam and Telangana. In 2022, among the 14,409 cybercrimes committed against women, 3,904 cases were from Karnataka, followed by Maharashtra with 2,530 cases. The following Chart 1.2 outlines the most vulnerable states which have reported the highest number of crimes against women in India from (2018-2022)[22]

2.1.2 State-wise analysis reporting the highest number of cybercrimes against women in India



Source: National Crime Records Bureau (NCRB) 2018 - 2022

The above five states such as Karnataka, Maharastra, Uttar Pradesh, Telangana, and Assam reported the highest number of cybercrimes against women as compared to the other states in India in the last five years. According to a survey, Karnataka had a higher-than-average rate of digital penetration and the highest number of official cybercrimes against women. However, Uttar Pradesh had lower than average digital penetration and the lowest incidences of cybercrime against women. Regardless of this fact, gender-based violence is noteworthy in Uttar Pradesh, where victimization is widely prevalent, even with a lower rate of digital

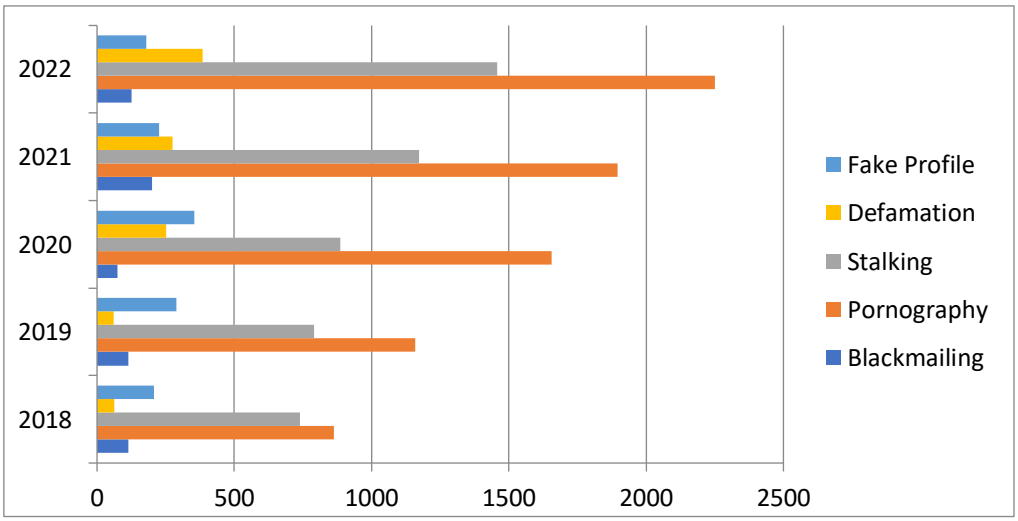
[21] Internet and Mobile Association India, *Internet in India Report(2022)* < https://www.iamai.in/> accessed 20th March,2024
[22] Supra Note 6

penetration. This demonstrates a significant underreporting of cybercrime against women, making it a serious concern.[23]

2.2 Types of Cybercrime against Women

In a society often characterized by patriarchal norms, women have always faced the highest vulnerability to crime. With the rapid advancements, the digital age has spawned new threats, which symbolize a continuous need for addressing women's safety in all spheres. There are various types of online threats that women face in this digital era, and the rampant usage of mobiles, the internet, computers, etc. has made women most vulnerable to these crimes. If we look at the wider aspect, cybercrimes are already a major threat in this ever-expanding digital age, and due to gender bias, women are mostly targeted in these crimes. Crimes related to sexual exploitation, pornography, and publishing obscene imagery are the most common types of crime that are seen against women. According to a European Report, 93% of image-based sexual violence was committed against females where victims have gone through serious emotional distress.[24] According to the NCRB data, in 2021 1,896 cases of sexual-exploitation against women were filed, and in 2022 the number rose to 2,251, representing an 18% increase. [25] The following Chart 1.3 shows the rise of different types of cybercrimes against women over the past five years (2018-2022).

Incidence of different types of cybercrime against women



Source: National Crime Records Bureau (NCRB) 2018 - 2022

[23] T. Sippy, U. Hembram, A. Durani, S. Chandiramani, *'Institutional Responses to Digital Harm: A case study of India's public and private institutional response mechanisms to tech-facilitated gender-based violence' (2023)* accessed < https://artha.global/wp-content/uploads/2023/01/WP_Institutional-Responses-to-Digital-Harms-1.pdf> 22nd March, 2024

[24] European Women's Lobby(EWL) Report, '*Her Net Her Rights*' *(2017)*

[25] Supra Note 6

Crime related to pornography has been consistently rising over the past few years against women. However, with technological progression, new types of crimes are also seen to be emerging such as deep fakes, non-consensual intimate imagery, online mobbing, etc. seen to be uprisings, which are specifically designed to exploit women.[26] Therefore, the most common types of cybercrime against women are cyber defamation, stalking, blackmailing, pornography, and cyber-sex trafficking and identity theft.[27] However, this broader category also encompasses various other crimes such as doxxing, digital voyeurism, E-mail spoofing, cyber grooming, cyber morphing, etc. under its ambit.[28]

2.2.1 Cyber Defamation

Cyber-defamation can be referred as the act of spreading false, defamatory content about an individual or entity online, commonly termed as online or internet defamation. This crime involves both libel and slander, where individuals or a group of individuals, either intentionally or unintentionally, defame a person in cyberspace. Though this type of crime can be committed against any person, irrespective of gender, women are the most vulnerable to this crime.[29] This type of crime is primarily committed on social media, where miscreants, by hacking someone's Facebook, Twitter, or email i.d., circulate malicious or defamatory messages to others to cause harm to the victim. Cyber defamation against women includes spreading rumors or lies online, posting manipulated images online, creating fake social media profiles, etc. These types of defamatory attacks against women are often sexist or misogynistic.[30] Therefore the various types of cyber defamation targeting women are:-[31]

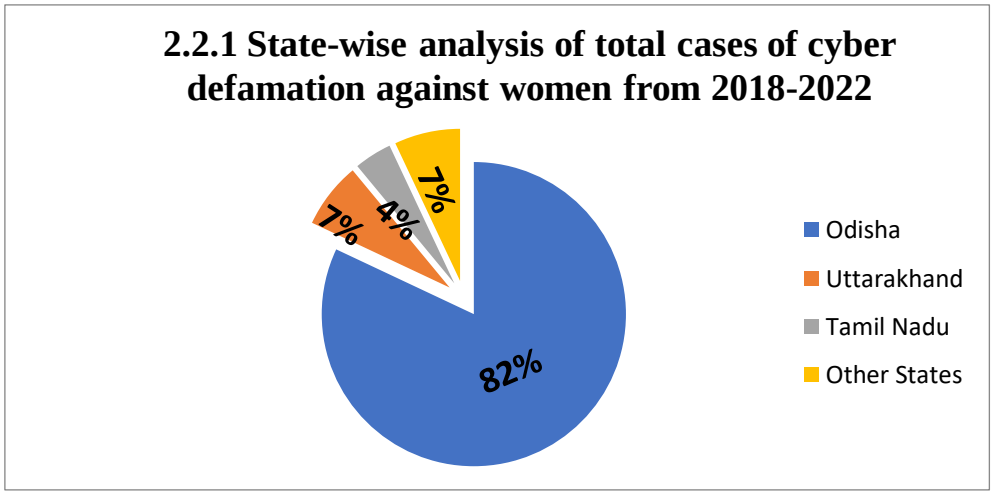
a. **Cyber Morphing: -** This refers to the digital manipulation of a person's image to create a false representation of someone. Cybercriminals use photo editing tools to alter a person's existing image to defame them. This involves the manipulation of a person's face into another person's body to make them appear different. It is seen that girls and women are the most vulnerable to these crimes.

[26] Ibid.
[27] Priya Gupta, *'Cybercrime against women in Indian context: An Overview'(2020)* 8 JRHSS 75
[28] Supra Note 14
[29] Supra Note 8
[30] Dr. Monika Jain, *'Victimization Of Women Beneath Cyberspace In Indian Upbringing' (2017)* Bharti Law Review, April- June 1
[31] J. Lakshmi Charan, A. Kumar Yagati, 'A Critical Analysis on Cyber Defamation In India: Laws and Issues in Present Scenario' (2023) 12 ECB 192 <https://www.researchgate.net/publication/372787994_> accessed 23rd March, 2024

b. **Revenge Porn: -** The goal of revenge porn is to make the victim feel degraded, harassed, and distressed. A person's right to privacy is violated when private and personal photos or films are distributed without their consent, a practice known as revenge porn. Criminals frequently perpetrate this kind of crime in order to harm their reputation.

c. **Hate Speech: -** The use of insulting, derogatory, and discriminatory language against an individual based on their gender, race, religion, etc. is known as hate speech. These kinds of languages are used to harm a person's reputation and well-being, causing them emotional, mental, and social distress.

The offense of defamation is generally penalized under 'Section 469' of the IPC, which speaks about 'forgery for purpose of harming reputation' and stipulates "imprisonment for a term extending up to 3 years or a fine". Additionally, several offenses, such as cheating by personation, violation of privacy, and transmitting obscene materials, are penalized under Sections 66D, 66E, and 67 of the IT Act, 2000, respectively, which form a part of cyber defamation.[32] According to the NCRB Data, over the past five years, i.e., from 2018 to 2022, a total of 842 cases of cyber defamation against women were filed in Orissa, followed by Uttarakhand with 77 cases and Tamil Nadu with 44 cases, making them the most vulnerable states in India. The following graph 2.1.1 represents a state-wise analysis of the total number of cases of cyber defamation or morphing against women from (2018-2022)[33]



Source: National Crime Records Bureau (NCRB) 2018 - 2022

[32] Ibid.
[33] Supra Note 6

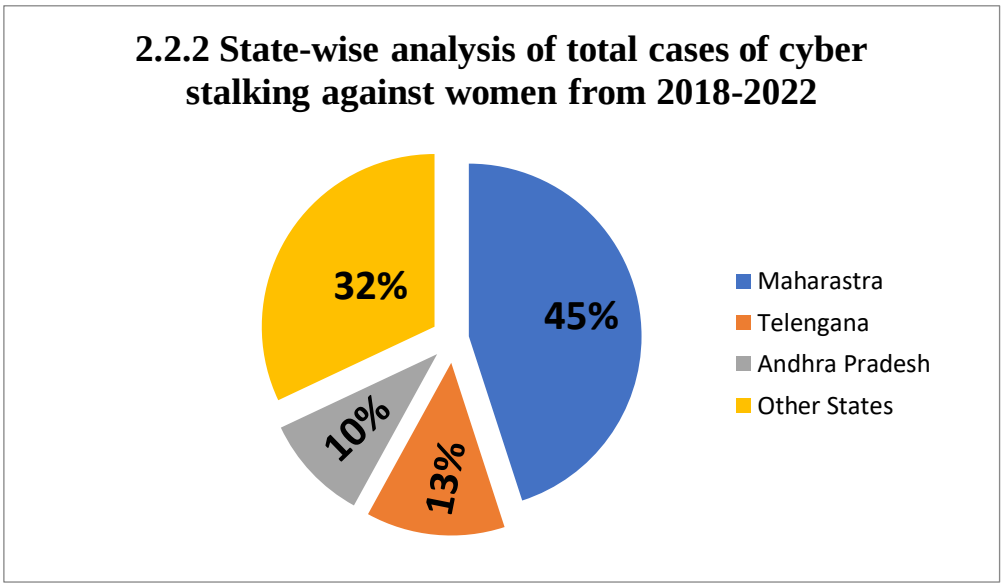
According to a survey by the Centre for Innovative Public Health Research, 26% of women between the ages of 18 and 24 fall victim to defamation and false rumors. The Digital Citizens Alliance reported that 61% of victims of online defamation are female, making women more likely than men to be targets of these attacks.[34] People in this digital age often encounter some type of online defamation, but women are disproportionately likely to be victims of these crimes.

2.2.2 Cyber Stalking

The term 'stalking' refers to the repeated behaviour of unwanted contact or attention to make a person feel unsafe or harassed. Cyberstalking refers to the situation in which criminals intimidate or threaten the safety and well-being of another person with the use of the internet and electronic mediums, including social media sites, emails, phone calls, text messages, etc. Cyberstalking against women includes spying, tracking a woman's online activities, sending threatening messages, harassing her with obscene materials, etc., which can have a devastating effect on a woman's life. Cyberstalking is a challenging issue as this crime doesn't have any geographical restrictions or physical confrontations; it may be caused by anyone from anywhere around the world. Additionally, stalkers maintain a high level of anonymity, which makes it difficult to identify or track the person causing harm.[35] Studies indicate that these crimes affect a woman's psychological and emotional state, often leading to feelings of fear, anger, depression, PTSD, and suicidal thoughts among victims.[36] Women's life is negatively impacted by the attitude towards them, especially those who are the victims of cyberstalking and are afraid of social shame and ruining their family's reputation they are less likely to report these crimes. People are less aware of the seriousness of cyberstalking they are not aware enough to accept that in this technological era, it's often likely to fall victim to cyberstalking. In this patriarchal society, women victims of cyberstalking are further victimized due to the gender-biased approach towards them.[37] Cyber Stalking also includes crimes such as cyber harassment, cyberbullying, voyeurism, etc. The crimes of voyeurism and cyber stalking are penalized under sections 354C and 354D of the

[34] Cyber Assurance Platform, *' Top 10 Cyber Crime against Women'(2024)* < https://xiotz.com/top-cyber-crime-against-women/> accessed 23rd March,2024
[35]Ms. Heena Keswani, *'Cyber Stalking: A critical study' (2017)* Bharti Law Review, April- June 131
[36] European Institute for Gender Equality(EIGE) *'Cyber Violence against women and girls key terms and concepts'(2018)* < https://eige.europa.eu/> accessed 23rd March,2024
[37] Ameema Miftha, Marcia Gibson *'Cyber Stalking is a Social Evil: From the Indian Women's Perspective'(2019)* 17th International Conference e – Society < https://www.researchgate.net/publication/334553216> 1st April,2024

'Indian Penal Code'. Section 354C deals with voyeurism which states that "anyone who witnesses or records a woman doing a private act without her knowledge or consent shall be punished with imprisonment which would extend to 3 years or with a fine". Section 354D, which covers 'stalking,' outlines that a man who continues to pursue or contact a woman, even after she clearly shows disinterest, shall be penalized with imprisonment for 3 to 5 years and a fine.[38] The NCRB data reported a total of 1,457 cases of cyberstalking in 2022, which resulted in a 24% rise from 2021. Maharashtra reported the highest number of total cases of cyberstalking with 45% in the last five years, i.e., from 2018 to 2022, followed by Telangana with 13% and Andhra Pradesh with 10%. The following graph 2.2.1 shows a state-wise analysis of the total number of cases of cyberstalking or bullying against women from (2018-2022)[39]



Source: National Crime Records Bureau (NCRB) 2018 - 2022

Regardless of a person's gender, stalking is a very severe problem in society that can happen to both men and women. But compared to men, women are twice as likely to experience stalking. Compared to less than 1% of men, about 1.8% of women reported having experienced stalking. It has been discovered that 67% of stalking victims frequently know their stalker, and that stalkers are frequently the victim's personal relationships.[40] Therefore, the online intrusion of a woman's privacy is recognized as cyber-stalking and various

[38] Sneha Mahawar, *'Overview of the concept of cyber bullying in India'(2023)* <https://blog.ipleaders.in/overview-of-concept-of-cyber-bullying-in-india/> accessed 1st April,2024
[39] Supra Note 6
[40] Max Sheridan, *' The Latest Cyber stalking Statistics for 2024' (2024)* <https://www.safehome.org/data/cyberstalking-statistics/#references> accessed 3rd April, 2024

psychological factors cause perpetrators to commit such crimes as obsession, religious fervor, mental disorders, sexual misconduct, erotomania, etc. The victim of this crime goes through severe physical and mental distress; hence it is important to keep the victim's welfare in mind while penalizing the perpetrator of this offence.

2.2.3 Cyber Blackmailing

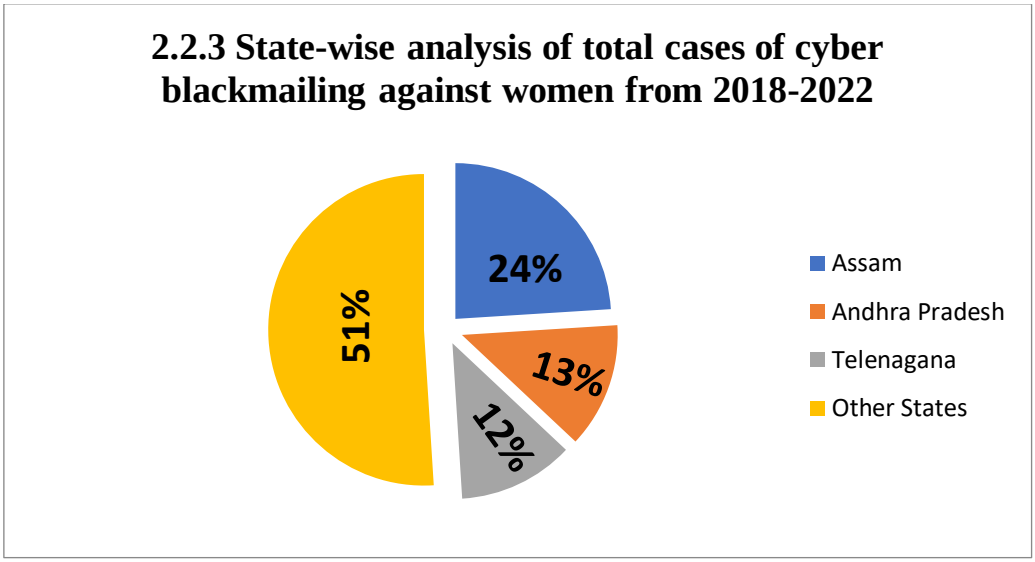
The term cyber blackmailing also known as cyber extortion or online blackmail is a type of cybercrime where a perpetrator threatens to disclose confidential information about a person unless certain demands are met. Blackmailers often carry out various tactics such as sending threatening emails, and messages, making phone calls, etc. to fulfill their demands. Cyber blackmailing can be done on various social media platforms, emails, through mobile phones. This type of crime can be of various forms such as emotional blackmail, financial blackmail, moral blackmail, electronic blackmail, etc. which has various psychological, physical, security, and social effects.[41] Blackmail on social media platforms has been a very common issue, and it also involves online self-disclosure, where victims share their personal and sensitive information with the perpetrators. Females and younger people between the ages of 15 and 25 are more likely to be victims of blackmail. Women are the most vulnerable, as it is very easy to threaten and blackmail them to get them to upload explicit and sexualized content. Other factors, such as lack of legal knowledge, greater usage of social media platforms, easy access to the internet, etc., also increase a person's vulnerability to being a victim of blackmail.[42] Therefore the various types of cyber blackmailing are as follows:-

a) **Cyber extortion: -** This is a sort of internet blackmail when the attacker threatens to publish the victim's private information, sexual photos, or videos until their demands are fulfilled. The victim of this type of crime may experience severe psychological suffering, such as anxiety, dread, and shame.
b) **Cyber doxxing:** - This is is a newly growing crime against women in which criminals threaten or extort someone to reveal private or sensitive information online. It is the practice of doing research and making private information publicly available

[41] M. Hassan Mekkawi, ' *Cyber Blackmail between threats and protection: A study of the Egyptians and American Legislations' (2022)*< https://jolets.org/ojs/index.php/jolets/article/download/71/23> accessed 4th April,2024
[42] Al Habis, M. Percy, *'Blackmail on social media: What do we know and what remains unknown?'(2021)* <https://pureadmin.qub.ac.uk/ws/portalfiles/portal/202125371/Accepted_Article.pdf> accessed 4th April,2024

online without the subject's consent. Doxxing, which includes online self-disclosure, frequently takes place on social media sites, internet forums, etc.

However, women also face various other types of cyber blackmailing in cyberspace, such as financial fraud, reputational damage, etc. Though these types of crimes can be committed irrespective of gender, women are seen as victims as they are the most soft targets and also due to the chauvinistic societal approach. According to the NCRB data, states like Assam, Andhra Pradesh, etc. are the most vulnerable states in India which experience cyber blackmailing due to a lack of knowledge about the consequences of the internet and also due to lack of legal implications. The following chart 2.3.1 shows a state-wise analysis of the total number of cases of cyber blackmailing against women from (2018-2022)[43]



Source: National Crime Records Bureau (NCRB) 2018 – 2022

The crime of sextortion is the highly committed crime of cyber blackmailing and the victim goes through mental, physical, and monetary loss. According to a report, the Maharashtra cyber police had stated that 42% of the registered cases are found to be cases of sextortion.[44]

[43] Supra Note 6

[44] H. Mondal, M.R. Sahoo, 'Characteristics of Cyber Sextortion in India: Content Analysis of online newspapers published in 2019-2021' (2022) < https://journals.sagepub.com/> accessed 4th April, 2024

2.2.4 Cyber Pornography

The term pornography comes from the Greek word "porne graphs," where "graphics" means to describe or write about prostitution and "porne" means to engage in it. The term "cyber pornography" describes the production, sharing, or exhibition of sexually explicit images or movies via digital platforms like computers and the internet. Cyber pornography also synonymous with cyber obscenity is one of the highly committed crimes against women in cyberspace. Cyber pornographers for their enjoyment distribute morphed images and obscene photos of women to blackmail or intimidate them. The victims of this crime are often subjected to revenge porn where the miscreants are often the ex-partner or individuals who have obtained images or videos from previous relationships which are further used to disseminate them across cyber space. However, images can also be obtained from hacking into a person's computer or mobile phone with the intent to harm their social life. According to a survey, 90% of revenge porn victims are found to be women.[45] The survey by the UK Charity Refugee, 2020 stated that 27% of men and 43% of women share intimate images while in a relationship. These intimate images pose a serious threat as they are distributed later on by their partners with the motive of revenge. Women are the most vulnerable victims of this crime as they can be manipulated emotionally very easily. In India, people are not very aware of revenge pornography. Studies have shown that most people have not heard of the phrase 'revenge porn' and are not sure whether pornography should be banned or not.[46] As the digital era is evolving, perpetrators are using recent technological developments to commit such crimes. Deep fake pornography is one such example where perpetrators use AI algorithms to morph sexually explicit images. Therefore, the various types of cyber pornography are:[47]

a. **Non-consensual pornography:** This is also known as revenge porn where sexually explicit images or videos are shared without the consent of the individuals. These types of images or videos are shared often to cause harm, embarrassment, or distress to the person. These types of crime often disproportionately affect women and they are targeted for various reasons such as misogyny, control, intimidation, etc.

[45] European Institute for Gender Equality, ' *Cyber violence against women and girls'* <https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf> accessed 4th April, 2024

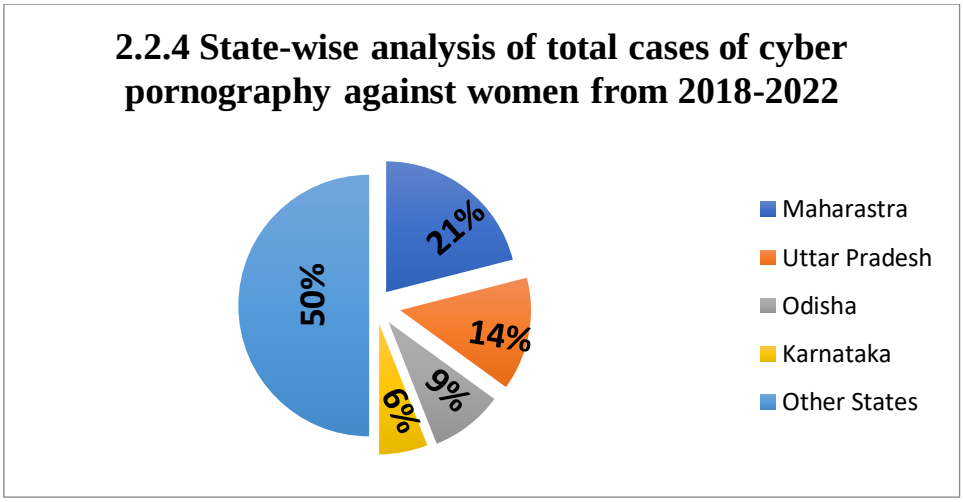
[46] M. Mathew, Vijayasarathy, *' Revenge Porn: A peep into its awareness among the youth of TamilNadu, India' (2023)* 11 IJIP 208

[47] B. Sinha, R. Sharma, *' Cyber Pornography in India: A Legal Insight'(2018)* 5 JETIR 203

b. **Deep fake pornography**: - This type of crime has been recently in trend with the evolution of artificial intelligence. Deep fake Pornography refers to the use of machine learning techniques and artificial intelligence to create realistic but fake pornographic content. This type of crime also falls under the purview of non-consensual pornography however in this crime fake morphed images are created. Victims of these crimes face the same consequences as those of non-consensual pornography.

c. **Virtual Sexual Assault: -** This type of crime refers to instances where individuals are sexually harassed, abused, or violated virtually in cyberspace. This includes sharing unwanted sexually explicit images, pressuring individuals to engage in sexual activities, passing sexual comments, displaying obscene images, etc. Victims of this crime often go through emotional distress, post-traumatic stress, etc.

The crime of cyber pornography has been consistently rising for the past few years. A total of 1,896 cases were filed in 2021, which rose to 2,251 cases in 2022, resulting in an 18% increase. With the new advancement of technology, new types of crimes are also emerging, and women in cyberspace are predominantly targeted by this specific offense and are sexually exploited. According to the NCRB data, Maharashtra is the most vulnerable state which has experienced 21% of cyber pornography against women in the last five years followed by Uttar Pradesh. The following graph 2.4.1 shows a state-wise analysis of the total number of cases of cyber pornography against women from (2018-2022)[48]



Source: National Crime Records Bureau (NCRB) 2018 – 2022

[48] Supra Note 6

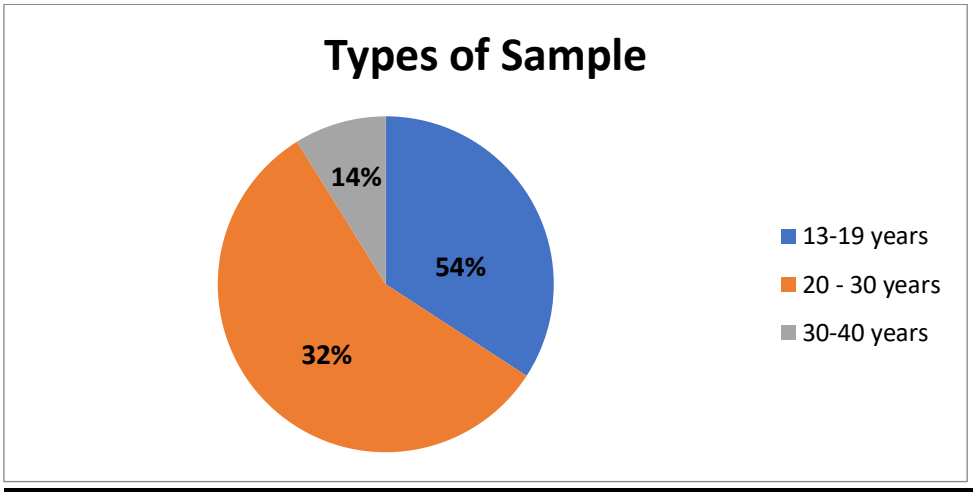
The Information Technology Act, 2000', particularly Sections 67 and 67A, which make it illegal to publish or transmit pornographic material, regulates cyberpornography in India. In order to regulate the unsuitable representation of women or any part of their bodies in entertainment, the media, etc., the Indecent Representation of Women's Act of 1986 was passed. Section 292 of the Indian Penal Code, 1860, describes the penalties for disseminating pornographic materials. Despite the fact that internet pornography is illegal in India under a number of statutes, new and efficient laws are required to prevent such crimes.

2.3 Data Analysis

I have conducted an empirical study involving 50 participants consisting of women of different ages and also women victims of cyber-crime. Below is a detailed analysis of the questionnaires administered and the responses received.

2.3.1 Sample Design:

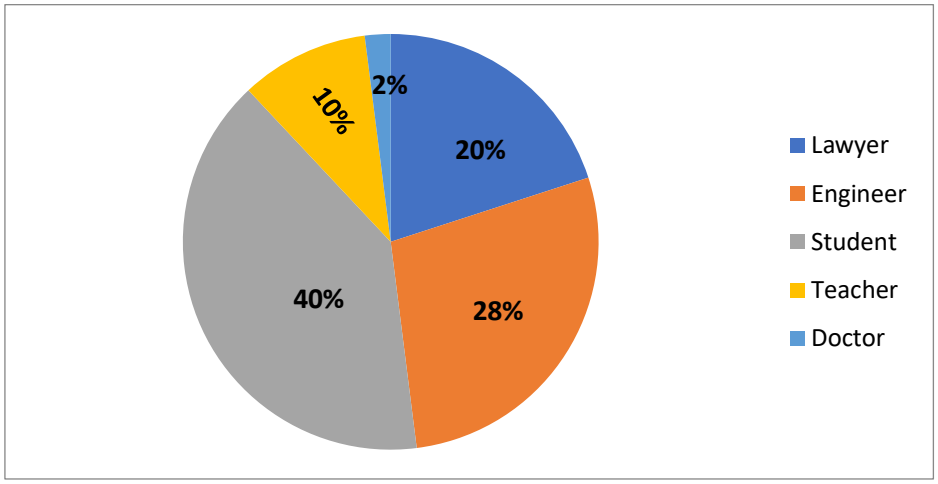
1. **Cyber Crime Victims**
2. **Women of Different ages**
3. **Group of 50 people**



A total of 50 samples were collected based on the convenience sampling method out of which 27 women belonged to the age group of 13 – 19 years, 16 women belonged to the age group of 20 – 30 years and 7 women belonged to the age group of 30 – 40 years. Therefore, 54% of women or girls belonged to the adolescent group and more than 30% were adults.

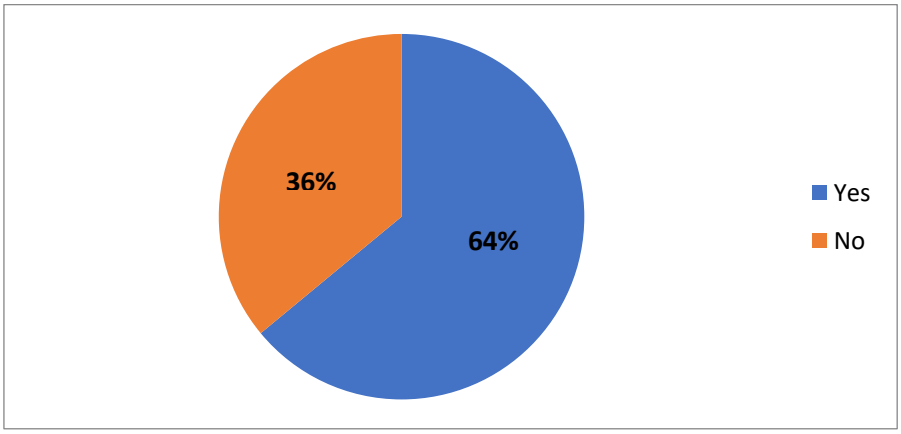
2.3.2 DETAILED ANALYSIS OF RESPONSES MADE TO EACH OF THE QUESTIONS IN THE QUESTIONNAIRE

1) Which profession do you belong to?



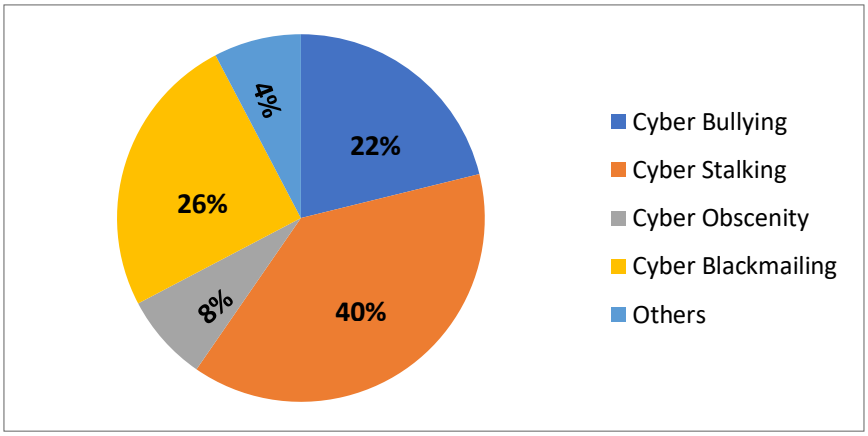
Among the 50 individuals, 40% of women i.e. 20 individuals of them were students, 28% of women i.e. 14 individuals were engineers, 20% of women, i.e. 10 individuals were lawyers, 10% of women, i.e. 5 individuals were teachers and 2% of women, i.e. 1 individual were doctors. Therefore, it has been observed that regardless of any profession, women falls victims of cyber-crimes in the digital space. Today in the 21st century, where we talk about the empowerment of women, increased rates of crime against women are still reported and even in the digital sphere they are not spared.

2) Whether you have faced any Kind of Cyber Crime?



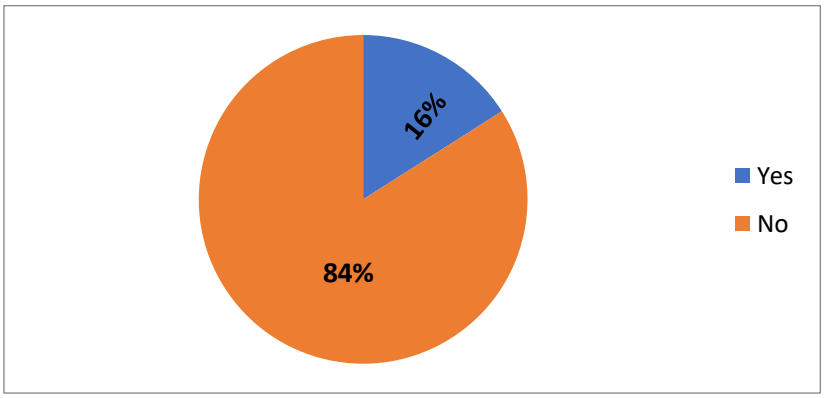
Among the 50 samples or women, 32 of them have reported that they have faced a certain form of cyber-crimes and 18 of them have reported that they have never faced any form of cyber violence. Therefore, more than 50 % of women reported that they have faced a certain form of cyber-crime against them which is a very concerning issue.

3) What Kind of Cyber Harassment have you faced online?



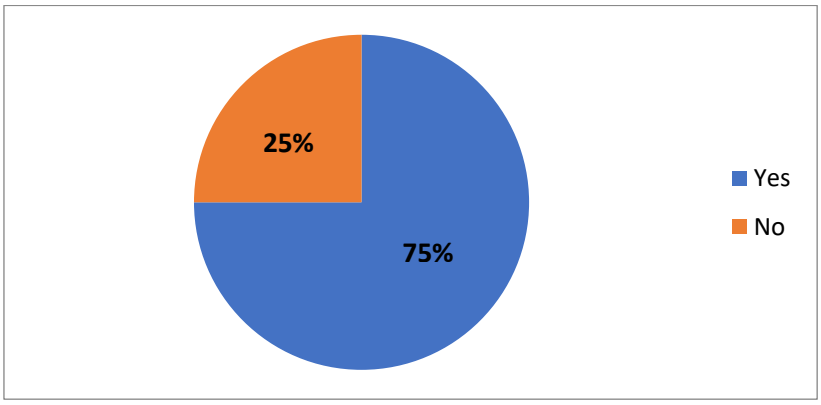
Among the 50 samples that were collected, 20 women reported experiencing cyber-stalking, making it the most commonly reported cybercrime, 13 women reported that they have been victims of cyber-blackmailing, 11 of them reported of Cyber Bullying and 4 women reported of Cyber Obscenity. However, crimes like Cyber Stalking and Cyber Blackmailing is the highest reported cyber-crime against women.

4) Have you filed a police Complaint?



Shockingly, among the 50 women mostly stated, that they have not filed a police complaint. The data shows, that 42 of them have stated that they have not filed a police complaint and only 8 of them have filed a complaint. The data therefore reveals an alarming issue that due to societal stigmas there are various complaints that are unnoticed. Though the cyber-crimes reported against women, poses a significant threat as it has been alarmingly rising since the past years. It can be undoubtedly stated that out of the books, there are numerous women victims who have faced some kind of cyber-threats online which goes unreported or unnoticed.

5) **If you have filed a complaint, did the police take any action against the accused?**



However, among the women who have reported that they had filed a police complaint, majority have stated that the police have taken action against the accused which shows a positive trend in combatting cyber-crimes against women. Among the 8 individuals who had filed a complaint, 6 of them have stated that the police have taken action against the accused and only 2 of them has stated no. This brings forward that even if there are high rates of cyber-crimes reported against women, the legal stakeholders are playing a vital role in controlling such crimes.

CHAPTER:- 3

CYBER FORENSICS IN THE ERA OF DIGITAL TRANSFORMATION: ASSESSING IT'S ROLE IN INVESTIGATING CYBERCRIME AGAINST WOMEN

The panorama of criminal activity has changed significantly in the age of digital technologies, creating special difficulties for the criminal justice system in controlling these types of crimes. The most important foundation for resolving cases and providing victims with justice is the examination of cases and supporting documentation. Since cybercrimes are frequently perpetrated via digital channels like social media, emails, and phone calls, it is very difficult to track down the perpetrator because they are not physically present. Cyber forensics, also known as digital forensics, is essential for locating criminals via digital means and guaranteeing that reliable evidence is gathered for the case. The field of forensic science known as "cyber forensics" has been developing quickly in recent years due to technological advancements.[49] Recently, there has been an increasing emphasis on digital forensics within the field of computer forensics, particularly in the context of preventing and prosecuting computer crimes, before computer forensics had to go through robust processes and techniques and therefore, many computer crime cases remained unsolved. Numerous factors contributed to the failure to prosecute these crimes, with a significant one being the lack of proper tools and skills among authorities to successfully collect digital evidence.[50] In the current scenario, with the introduction of this branch of forensic science, tracing of criminals has come significantly within our reach yet posing different other challenges. In the present situation, computer forensics must guarantee that evidence is taken from a computer without destroying the original damning material and must bring unity and uniformity to this wide sector.[51]

A high level of expertise is required for the extraction of digital evidence, and during investigations, a reliable chain of custody must be carefully maintained. While there are many opportunities brought about by modern technology breakthroughs, there are also many obstacles. Nowadays, a computer, phone, or other electronic gadget is more likely to be the

[49] P. Maravic & S. Bosnjak, *'Cybercrime and Digital forensics: Technologies and Approaches'* (1st edn. DAAM International Scientific Book, 2014)
[50] Ibid.
[51] Ibid.

"smoking gun" than a conventional weapon.[52] Digital forensics has been a boon in the criminal justice system to control different cybercrimes. The importance of digital forensics can never be ignored as it plays ninety per cent role in most of the criminal cases. According to the stakeholders and investigators of digital forensics, states that it offers significant benefits such as swift and fast justice, prevention of numerous future crimes, reduction in the duration of investigations, and lowering of court costs.[53] The field of cyber forensics in combatting cybercrime against women primarily concentrates on extracting digital evidence, tracing criminals within cyberspace, and plays a crucial role in removing content for individuals who have fallen victim to revenge porn.

3.1 What is Cyber Forensic?

The word "forensic" comes from the Latin word "Forensis," which usually means "of or before the forum." The application of scientific concepts and methods to criminal investigations and legal issues is the focus of the forensic science field.[54] Cyber forensic also commonly known as digital forensic or computer forensic began to take shape in the late 20th century as computers and digital technologies became more widespread. Although this branch of forensic science has gained more prominence in recent years, its origins can be traced back to the late 1970s. Michael Anderson is one of the early pioneers in this field who used a computer to investigate crimes in those times. His work is often cited as one of the first examples of computer-based forensic investigations.[55] Soon after, in 1986, Clifford Stoll used computer forensic technologies to track down a hacker who was breaking into U.S. military and government computers. His research, which was published in his book The Cuckoo's Egg, made clear how important it is to have specific tools and methods in order to look into digital crimes. In order to gather and preserve evidence from a computer device that is appropriate for presentation in a court of law, cyber forensics uses specialized examination and analysis procedures. Cyber forensics' major goal is to carry out a comprehensive investigation while keeping a meticulous chain of custody, pinpointing exactly what was

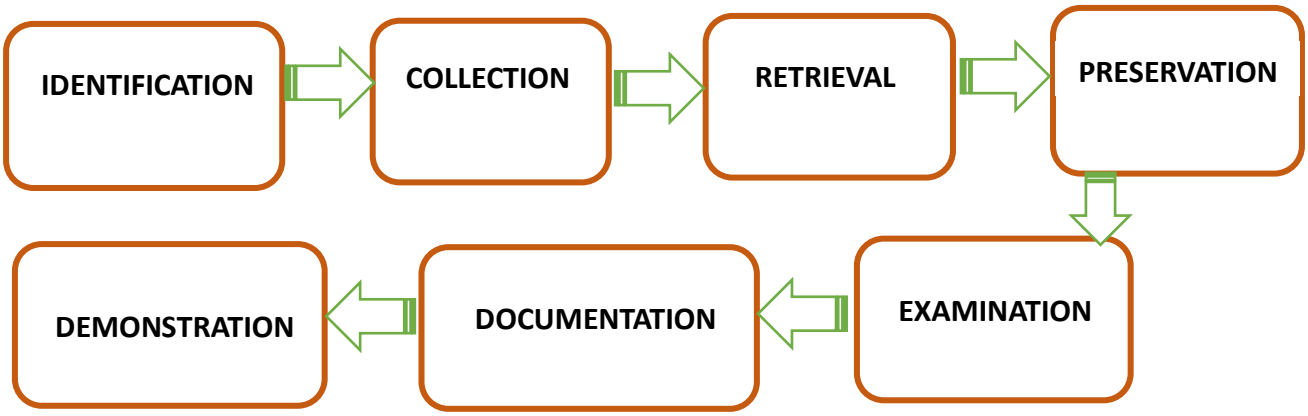
[52] M. Gunawardhana, *'Role of Digital Forensic in solving cyber crimes'* (2021) <https://www.researchgate.net/publication/360919194_Role_of_Digital_Forensic_in_solving_cyber_crimes> accessed 15th August, 2024

[53] R. Muir, S. Walcott, 'The Police Foundation UK, 'Unleashing the value of digital forensics' (2021) <https://www.police-foundation.org.uk/wp-content/uploads/2010/10/value_of_digital_forensics.pdf>accessed 15th August, 2024

[54] Nyayags Society of Forensic & Criminal Justice. 'Digital Forensics and Legal Aspects' <https://nyayags.org/digital-forensics-and-legal> accessed 16th August, 2024

[55] Suwarna Nimkarde, Shobhana Gaikwad, 'Digital Forensics' 11 IJARCEE 703

discovered on the device and identifying the accountable party.[56] The cyber forensic investigation process includes the following important steps:



To maintain a proper chain of evidence, first we need to identify the evidence that where and how it is stored then the collection phase involves gathering the identified digital evidence in a manner that maintains its integrity. Thirdly, the evidence is then extracted from the identified device by a forensic investigator and to maintain its integrity the original evidence is preserved. The process of examination is the most important part as this step includes the evaluation of the evidence to identify its relevancy to the case and is then interpreted and documented in an easy manner and finally it is demonstrated and is presented in respect to the case in front of the court. To present the best evidence in front of the court an investigator must prepare detailed documentation that includes the chain of custody and evidence analysis and this evidence will then be subjected to scrutiny by the opposing party.[57] Therefore, the branch of cyber-forensics is a response to cybercrime to investigate if anything adverse has happened and also to determine the source of incident, the associated damage and to recover the data.[58]

3.2 Classification of Cyber Forensic:

The branch of Cyber Forensics can be classified in the following:[59]

3.2.1. Network Forensics: This branch focuses on monitoring and analyzing network traffic to detect and investigate cyber-attacks, unauthorized access, tracing criminals and

[56] Aparna Chaturvedi, A. Awasthi, S. Sanker, *'Cyber Forensic – A literature Review'* 10 TJMIM 24
[57] Dejey Murugan, *'Cyber Forensics'* (Oxford University Press, 2018)
[58] Iid.
[59] Padmavathi Ganapathi, 'Digital Forensics and Investigation Methods' (Notion Press, 2022, Pg: 56-60)

other malicious activities. It involves collecting and analyzing network logs and other network-related data to get access to the digital footprints of the perpetrator.

3.2.2. Mobile-device Forensics: This branch of forensic pertains to the recovery of digital evidence from mobile devices, including smartphones and tablets. It covers data such as call logs, text messages, GPS data, photos, and application data, which can be crucial in criminal investigations.

3.2.3. Computer Forensics: This involves the examination of data from computers, laptops, and storage devices. It aims to identify, preserve, recover, and analyze data to use in legal proceedings. This includes identifying the scope and type of digital evidence to be collected, such as hard drives, USB devices, or specific files.

3.2.4. Malware Forensics: This includes the study and analysis of malicious software to understand how it operates, spreads, and impacts a system. This type of forensics helps identify the nature of the malware and the intent behind its use, often providing insights into cybercriminals' tactics.

3.2.5. Cloud Forensics: This includes the investigation of data stored in cloud environments and retrieving digital evidence from cloud storage systems, which may include files, logs, user activities, and transaction records. However, cloud environments often distribute data across multiple locations and servers, making it difficult to identify and collect all relevant evidence.

3.2.6. Social Media Forensics: This branch includes the collection and analysis of data from social media platforms. This type of forensics is increasingly important in cases involving cyberbullying, harassment, and other online crimes.

3.2.7. IoT Forensics: This branch pertains to the investigation of data from Internet of Things (IoT) devices which includes smart home devices, wearable, and other connected gadgets. IoT forensics is emerging as a vital area due to the increasing use of such devices in daily life and potential involvement in crimes.

To address cases of cybercrimes targeting women, the branches of network forensics, mobile forensics, and social media forensics are most commonly employed. These specialized areas of cyber forensics play a crucial role not only in investigating cybercrimes but also in various

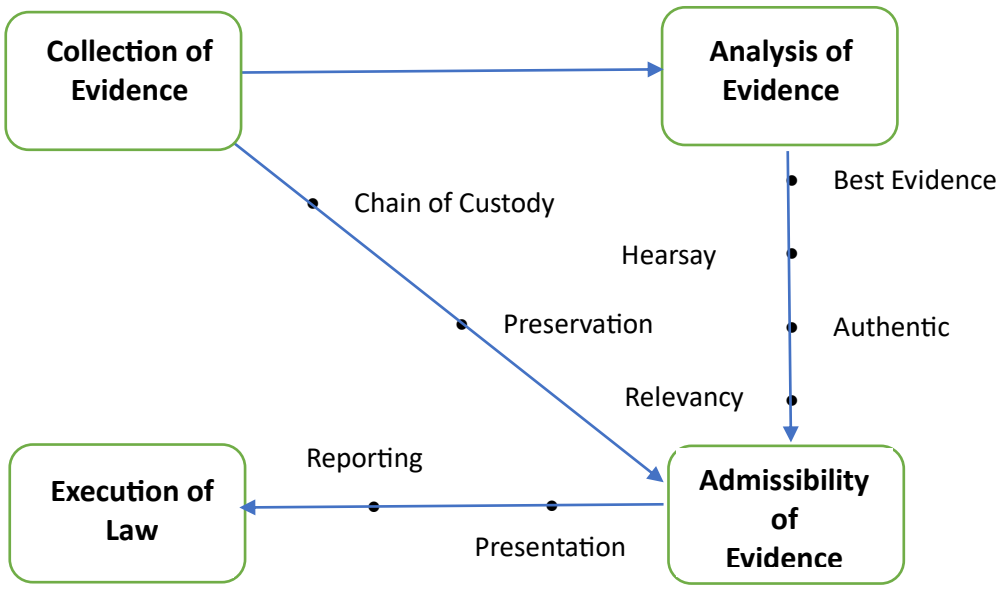
types of criminal cases. The significance of digital forensics has grown considerably, particularly in the 21st century, as criminals increasingly rely on online platforms where they can operate under a veil of anonymity. As a result, digital forensics has become an essential tool in modern law enforcement, helping to uncover and prevent crimes that occur in the digital realm.[60]

3.3. The Nexus Of Cyber Forensic And Digital Evidence

After the collection of the evidence device, the main aim of a forensic expert is to ensure the retrieval of the evidence from the device. Cyber forensics plays a crucial role in solving cases related to cybercrimes against women by providing a systematic and logical approach to collecting, analyzing, and preserving digital evidence.[61] Experts trace digital footprints left by perpetrators, such as IP addresses, emails, chat logs, and social media interactions, to identify suspects and even if the perpetrator tries to delete evidence, forensic tools can recover the deleted files.[62]The most common evidences that appears related to cyber crime against women are WhatsApp messages, phone calls and other social networking mediums. These evidences become hard to present in court as it requires a proper chain of custody to preserve these evidences in its original form in order to prevent tampering. Also, in certain cases a forensic expert testimony is required in court regarding the credibility of the digital evidence. Digital evidence to be admissible in court requires to be authentic, complete, reliable and believable. In the case of **Anvar P.V. v. P. K. Basheer & Ors,**[63] the Supreme Court of India held it mandatory that for digital evidence to be admissible in court requires a certificate under Section 65B of the Indian Evidence Act. The admissibility of these evidences requires certain technical and legal requirements and to make evidence admissible in court digital forensic experts are required to uphold the privacy and confidentiality of all individuals involved in the investigation. They must ensure that the methods used to collect and examine digital evidence do not infringe upon anyone's right to privacy.[64] The digital evidence also needs to meet certain technical aspects firstly, it should have a well-documented history of its

[60] C. Morgan Whitcomb, *'An Historical Perspective of Digital Evidence: A forensic scientist's view'* 1 IJDE 22 (2002)
[61] H. Sekhawat, D. Sabharwal, *'Digital Evidence and Cyber Forensic procedure and its Role in Criminal Justice System'* 9 PACCLAIMS 1 (2020)
[62] Supra Note 9
[63] Anvar P.V. v. P.K. Basheer & Ors (2014 10 SCC 473)
[64] R. Bharati, P. Khodke, *'Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings'* 11 IJSRST 24

handling and storage and secondly, the investigators must possess appropriate expertise, and the tools used for analyzing the evidence should be current and reliable.



Digital evidences serve as a paramount in cases related to cybercrime against women and therefore prevention of these evidences from getting tampered is very necessary. The landmark case of **Suhas Katti v. State of Tamil Nadu**[65] marked a significant development in the Indian judicial system by addressing the use of digital evidence for the first time. In this case, the accused was convicted for posting obscene messages about a woman on the internet, in violation of Section 67 of the Information Technology Act, 2000. This case was pivotal as it was the first instance where digital evidence was formally accepted in court under Section 65B of the Indian Evidence Act. In the case of **Shafhi Mohammad v. State of Himachal Pradesh,**[66] the Supreme Court stated that in certain circumstances, obtaining a Section 65B certificate may not be feasible. For instance, when the electronic evidence is not directly under the control of the person presenting it, the certification requirement may be relaxed. This ruling introduced flexibility in handling digital evidence, ensuring that justice would not be hindered by procedural technicalities.

Digital evidence is now integral to nearly all court proceedings and has been successfully used to prosecute offenders under both the Information Technology Act and the Indian Penal Code. Additionally, various courts have relied on electronic evidence to establish facts in both civil and criminal litigation and have admitted and evaluated electronic evidence in numerous instances. However, when electronic evidence is presented in court, its admissibility is first

[65] Suhas Katti v. State of Tamil Nadu (CC. No. 4680 of 2004)
[66] Shafhi Mohammad v. State of Himachal Pradesh, SLP(Crl.)No.2302 of 2017

established through a certification under Section 65B of the Evidence Act.[67] This scenario has taken a positive shift after the enactment of the new evidence act i.e. the Bhartiya Shakshya Adhiniyam, The **Section 2(1)(e)** which defines the term 'evidence' has included electronically given statements in the definition. Moreover, a new section i.e. **Section 61** is added in the act which states that the admissibility of digital or electronic record as evidence cannot be prevented solely on the basis that it is an electronic record and it shall carry the same legal effect, validity and enforceability as any other document. **Section 63**[68] of this act also speaks about the admissibility of digital evidence which has broadened the scope of e-evidence. This section allows for various forms of secondary evidence, but the emphasis remains on the admissibility of copies or substitutes for the original document, there are no specific requirements for a certificate like in Section 65B, but the authenticity and reliability of secondary evidence must be established and the court will assess the credibility of secondary evidence based on the circumstances under which it was produced. This section has a wide range and applies to all forms of secondary evidence, not limited to electronic records.

Although digital evidence can be used in various forms of criminal cases, tampering of the evidence still remains a concern. The essential requirements in to prevent evidence tampering are as follows:[69]

a) **Maintaining proper chain of custody:** Documentation of every step of evidence handling is an essential requisite to protect evidence tampering. This includes details like date, time, details of person accessed it, time of access, and purpose. This chain of custody must be meticulously recorded to prove that the evidence has not been tampered with or altered in order to get the evidence admissible in court.
b) **Hashing and Hash Verification:** Using cryptographic hash functions is essential to create a unique hash value for the original evidence. This technique is another essential perquisite to prevent tampering of e-evidence. The hash value of the digital evidence should be re-calculated after analysis to ensure that it matches the original hash, proving that the evidence has not been modified.
c) **Create forensic copy:** Immediately after the evidence is collected a forensic copy of the original data should be made using specialised tools. This process ensures that the

[67] Indian Evidence Act, 1872
[68] Bhartiya Shakshya Adhiniyam, 2023
[69] Supra Note 17

original data remains untouched while analysis. This process allows the forensic expert to analyze the e-evidence properly without tampering the original evidence and keeps the original copy secured.

Therefore, a cyber forensic expert plays a crucial role in the collection, preservation, and presentation of digital evidence. Since evidence forms the foundation for establishing the facts of a case and proving the elements of a crime, handling it properly is vital. The process of managing digital evidence is particularly challenging because any misstep can compromise its integrity. It is essential for a forensic expert to follow all legal protocols meticulously in the handling and analysis of evidence. Even a single loophole in this process can result in the evidence being deemed inadmissible, potentially leading to the release of the accused. As a key stakeholder in the justice process, the cyber forensic expert must ensure that the integrity of the evidence is maintained at all times, safeguarding its value in legal proceedings.[70]

3.4. Tools and Techniques Used for Investigating Cybercrimes against Women in India

Cyber forensic investigators and experts play a vital role in combating cybercrimes against women, with a particular focus on tracking down perpetrators and ensuring justice for victims. The investigation of such crimes requires specialized knowledge and tools, as offenders often exploit the anonymity and vast reach of the internet. Cybercrime against women in India is a growing concern and the government is also taking initiatives by establishing cyber forensic cum training laboratories with an aim to prevent such crimes.[71]

It has been found that criminals frequently target women in cyberspace primarily due to the anonymity the internet provides. This anonymity makes it easier for the perpetrators to commit these offenses without immediate repercussions. Alarmingly, in many cases, the perpetrators are found to be individuals from the victim's personal life, such as ex-partners, close friends, and even uncles.

The cyber forensic experts use various tools in order to investigate and track the perpetrators by following their digital footprints. These forensic tools are used for various purposes such as extracting deleted data, password recovery, ram analysis and many more. Mostly, in cases

[70] Supra Note 8

[71] National Commission of Women, 'Cyber crime prevention against women and children' < http://ncw.nic.in/ncw-cells/legal-cell/new-bills-laws-proposed/cyber-crime-prevention-against-women-and-children-ccpwc> accessed 17th August, 2024

of cybercrime against women various different tools are used to remove the obscene materials from different website for those who have been victims of online sexual harassment. The various kinds of investigating processes used in investigating cyber-crimes against women are:

3.4.1. Forensic Tools used for Data Recovery

Data recovery is the process of restoring or retrieving data that is corrupted, lost or damaged from the storage devices. This technique is employed when data becomes inaccessible through standard methods, whether due to corruption, accidental formatting, or damage to the storage medium. It is commonly used on devices such as SD cards, internal and external hard drives, SSDs, CDs, DVDs, and other forms of storage.[72] The process of data recovery is also used in cases of cybercrimes against women, where the perpetrators try to tamper with digital evidences by deleting data. Therefore, the tools used in recovering data are:[73]

1. **Recuva:** This software is a free user-friendly software which is used to recover data that have been accidentally deleted from a computer or external storage devices. This software can quickly recover files 'lost' due to system flaws, hardware failures, or malware infections. It allows data of any size to be retrieved within seconds, making it an efficient tool for recovering lost information. It can retrieve files from a variety of storage media, including hard drives, USB flash drives, memory cards, and even damaged or formatted disks.
2. **Encase:** This is a comprehensive digital forensics and data recovery software which is widely used by law enforcement agencies, corporate investigators, and cybersecurity professionals to gather, preserve, and analyze digital evidence. The key feature of this software includes file signature analysis, the ability to view deleted files and file fragments in unallocated or slack space, folder recovery, log file and event log analysis, as well as external file and registry viewers for comprehensive investigation and data recovery.
3. **Byte back:** This is a data recovery software which has a user-friendly interface, making it accessible for both beginners and advanced users. This tool supports multiple file systems and offers features like deep scanning for thorough file recovery and the ability to preview recovered files before restoring them. This tool also offers

[72] S. Tomer, A. Apurva, *'Data recovery in forensics'* 12 IEEE 188 (2017)
[73] S. N. Varayogula, K. Dodiya, *'Computer Forensics Data Recovery Software: A Comparative Study'* 10 IJIRCST 513 (2022)

write-blocking functionality for source drives, along with automatic CRC and MD5 hash calculation to ensure the accuracy of copy operations.[74]

3.4.2. Forensic Tools used for Mobile Devices

As mobile phones have become integral to daily life, they often hold key evidence in criminal cases, making mobile forensics a crucial part of modern investigative techniques. Mobile forensics is a branch of cyber forensics that is focused on the recovery, investigation, and analysis of data from mobile devices like smartphones and tablets. The tools used in this are:[75]

1. **MOBILedit:** This is a powerful mobile forensics tool widely used by investigators to extract, analyze, and manage data from mobile devices. This software allows access to contacts, messages, call logs, media files, and even deleted data, making it valuable in criminal investigations. One of its notable features is the ability to bypass device locks and encryption in certain cases, ensuring that critical evidence can be retrieved even if the device is secured.
2. **Belkasoft Evidence:** This tool is used to helps investigators extract, analyze, and examine data from mobile devices like smartphones and tablets and is widely used in cyber forensics to uncover crucial evidence stored on mobile devices. It supports the extraction of data from both Android and iOS devices and can analyze data from various mobile apps like WhatsApp, Facebook Messenger, Instagram, and many other applications.
3. **Cellebrite:** It is among the most widely utilized and highly regarded tools in mobile forensics, providing extensive solutions for data extraction, decoding, and analysis from mobile devices. It is the only handheld cellular exploitation device globally that operates without the need for a PC or additional phone drivers. The Cellebrite Physical Analyzer serves as the investigative platform, enabling examiners to perform keyword searches, bookmark relevant data, recover deleted information, and generate customized reports to aid their investigations.[76]

[74] Supra note 9
[75] M.Dweikat, *'Digital Forensic Tools Used in Analyzing Cybercrime'* 23 JUSST 367 (2021)
[76] Supra Note 9

3.4.3. Forensic Tools used for Password Recovery

Today, almost each and every file, devices and data are password protected and thus it becomes quite challenging for forensic experts to collect data. Therefore, investigators use certain tools to gain access to critical data that may be locked behind user authentication measures. Password recovery is essential in cases involving encrypted communications, secure databases, or personal devices that may contain vital evidence. Thus, the tools used for password recovery:[77]

1. **Passware Kit:** This is a powerful password recovery and decryption software widely used in cyber forensics, data recovery, and IT security. It enables users to recover passwords from various file types, such as Microsoft Office documents, PDFs, ZIP archives, and more. It minimizes the time required for password recovery, enhances success rates, and provides greater control over the recovery process.
2. **Ophcrack:** This is an open-source password recovery tool widely used in digital forensics, especially for cracking Windows passwords. It utilizes rainbow tables making it highly effective at recovering simple alphanumeric passwords in a short amount of time. Forensic investigators often rely on this tool due to its speed and efficiency, as it can quickly recover passwords without the need for brute force methods.

3.4.4. Forensic Tools used for Network Analysis

Network analysis in cyber forensics involves examining logs and connections between devices to identify and trace unauthorized access, and reconstruct the sequence of events that led to the crime. By analyzing networks, investigators can determine the origin of an attack, identify compromised systems, and even uncover hidden communications between cybercriminals. The tools used for network analysis:[78]

1. **Network Mapper (Nmap):** This is a powerful open-source tool widely used for network discovery and security auditing. This allows cybersecurity professionals and system administrators to scan large networks, identify active devices, and discover services running on a network by analyzing open ports. It uses raw IP packets to

[77] Dejey Murugan, *'Cyber Forensics'* (Oxford University Press, 2018)
[78] Supra Note 24

identify which hosts are active on a network, the services they provide, the operating systems they are running, and the types of packet filters or firewalls in place.

2. **Ethereal:** This is also known as Wireshark is a crucial tool in cyber forensics, particularly for network analysis. It functions as a network protocol analyzer that captures and examines data packets transmitted across a network. In cyber forensics investigations, especially in cases of cybercrime against women, such as identity theft, online harassment, or distribution of malicious content, Wireshark is essential for monitoring network traffic. Investigators can use it to detect suspicious activity, identify unauthorized access, and track data transmissions.
3. **Tripwire:** This is a powerful tool for detecting unauthorized changes within a network's infrastructure, playing a vital role in maintaining the integrity of network devices, servers, and configurations. It helps investigators monitor critical system files, configurations, and directories, alerting them to any suspicious or unauthorized modifications that could indicate a breach or malicious activity. It allows forensic experts to track changes that occur in real-time, helping them trace the source of the attack or breach.
4. **NetScout:** This is also a network performance management and cybersecurity tool widely used in network forensics to ensure the security, availability, and reliability of networks. In cyber forensics, it plays a critical role in monitoring network traffic, detecting potential security breaches, and analyzing malicious activities.

3.4.5. Forensic Tools used for Obscene Content Takedown

As internet usage grows and more content is shared across websites and social media sharing and publishing obscene content particularly with an intent to harass women has emerged as a concerning issue.[79]The process of obscene content takedown specifies various other processes such as social media monitoring tools, image and video analysis tools and legal takedown services. The tools used in this purpose are:

Image and video analysis tools:[80]

1. **Photo DNA:** This is a pioneering tool developed by Microsoft that plays a crucial role in combating the spread of obscene and illegal content online. This technology creates

[79] Upasana Borah, *'Cyber Crime Against Women in the Digital Era: A brief Indian Scenario'* 8 IJRASET 615 (2020)
[80] L. Sanchez, C.Grajeda, *'A practitioner survey exploring the value of forensic tools, AI filtering, & Safer Presentation for Investigating Child Sexual Abuse Material'* 29 DFRWS 124(2019)

a unique digital fingerprint for each image by analysing its visual features, allowing for precise identification even if the image has been altered, resized, or otherwise modified. It allows forensic investigators and other individuals to battle online exploitation, especially in protecting women and children from abuse.

2. **CAMS:** This is a specialized forensic tool designed to identify and categorize illegal and obscene content, particularly material related to child abuse and can be used for women also. It utilizes advanced algorithms and machine learning techniques to analyze and detect explicit content, ensuring that it is flagged and addressed appropriately. The tool scans through vast amounts of data to pinpoint images and videos that match known patterns or characteristics of abusive materials.
3. **Google Content Removal:** This tool is a service provided by Google to help individuals and organizations request the removal of specific content from Google search results and associated platforms like YouTube. This tool is particularly useful for addressing and managing harmful or inappropriate material, including obscene content, that appears in search results or on Google-owned sites.

3.4.6. Forensic Tools used for Social Media monitoring:

1. **Hootsuite:** This is a robust social media management tool that can be instrumental in addressing and managing obscene content on social media platforms. It allows users to set up streams to monitor specific keywords, hashtags, or mentions across various social media platforms. This feature is crucial for detecting and tracking the spread of obscene content, including harassment or explicit material targeting individuals.
2. **Follower work:** This is a social media management tool primarily designed to help users grow their followers and manage their social media accounts. While its main focus is on increasing engagement and follower count, it can also be leveraged to address and manage obscene content on social media platforms. This software allows users to track interactions and mentions related to their social media accounts. By setting up specific keywords or hash tags, users can monitor for obscene content or inappropriate behaviour directed at their profiles.

Therefore, these forensic tools are used widely in order to control cybercrime against women and play a crucial role in combatting the online threats of various cybercrimes.

3.5. Advantages of Cyber Forensics

Cyber forensics, also known as digital forensics comes with certain advantages such as: [81]

1. **Fraud Detection:** It helps in detecting and investigating fraudulent activities such as financial fraud, identity theft, and other cybercrimes. Cyber forensics has made the process fast and quick in finding the culprit behind the cyberspace.
2. **Regulatory Compliance:** Another significant advantage of cyber forensics is its contribution to regulatory compliance. Organizations are increasingly subject to a range of legal and regulatory requirements related to data protection, privacy, and cyber security. Cyber forensics plays a crucial role in ensuring that these obligations are met by providing a systematic approach to investigating and documenting security incidents.
3. **Legal proceedings:** Cyber forensics offers a substantial advantage in legal proceedings by providing reliable and admissible evidence essential for both prosecution and defence in cases involving digital crimes. In the realm of legal disputes, whether civil or criminal, the integrity and credibility of evidence are paramount. Cyber forensics ensures that digital evidence is collected, preserved, and analysed in accordance with strict protocols that uphold its validity in court.
4. **Training and Awareness:** Another notable advantage of cyber forensics is its role in enhancing training and awareness programs within organizations. The insights gained from forensic investigations into cyber incidents provide invaluable information that can be used to educate and train staff on cyber security best practices. This knowledge enables organizations to develop targeted training programs that address the specific weaknesses and threats identified during forensic investigations.

3.6. Challenges Of Cyber Forensics

Though the digital forensics comes with certain advantages, it is also crucial to speak about the drawbacks or disadvantages that the investigators or organisations face:[82]

[81] Global Security Network, *'Benefits and Challenges of Digital Forensics'* <https://globalcybersecuritynetwork.com/blog/benefits-and-challenges-of-digital-forensics/>accessed 14th august, 2024

[82] A.K Pandey, G. Kapil, *'Current Challenges of Digital Forensics in Cyber Security' <https://www.researchgate.net/publication/338756056>accessed 15th August, 2024*

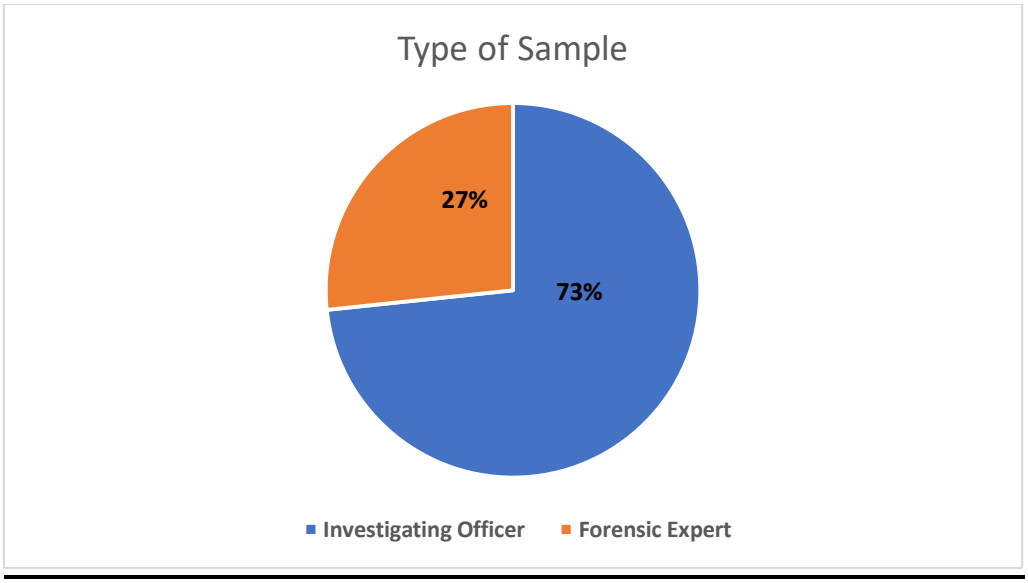
1. **Complexity of Data:** As the digital landscape expands, forensic investigators face a deluge of data generated from diverse sources like mobile devices, computers, cloud storage, and social media platforms. The volume of data makes it difficult for investigators to analyse relevant information. This often results in prolonged investigations and higher resource demands, as pinpointing critical evidence within massive datasets becomes more time-consuming and labour-intensive.
2. **Encryption and Anonymity**: The widespread use of advanced encryption technologies and anonymous networks creates significant barriers for forensic investigators. Encrypted data is often inaccessible and the anonymity of offenders is a serious challenge. It can pose threat for investigators to trace the origin or identity of suspects.
3. **Jurisdictional Challenges**: Cybercrimes often span multiple countries, with perpetrators, victims, and digital infrastructure located in different jurisdictions. This creates legal and procedural obstacles for forensic investigators, as laws, regulations, and enforcement capabilities vary across borders. These challenges can hinder timely investigations, allowing criminals to exploit gaps in global cybercrime laws and evade justice.
4. **Privacy Concerns**: The collection and analysis of digital evidence can raise significant ethical and legal issues related to individual privacy rights. When investigators access personal devices, communication records, or sensitive data, they risk infringing on privacy protections. The balance between acquiring crucial evidence and respecting privacy laws is delicate, especially in cases involving non-suspects whose data may be swept up in the process.
5. **Rapid Technological Changes**: The fast pace of technological innovation often surpasses the ability of forensic tools and methodologies to keep up. This gap can delay investigations, hinder the ability to address crimes involving cutting-edge technologies, and necessitate constant adaptation in the field of cyber forensics.

3.7. Data Analysis

I have conducted an empirical study involving 30 participants, consisting of cyber forensic experts and crime investigation officers, to examine the role of cyber-forensics in addressing cyber-crimes against women. Below is a detailed analysis of the questionnaires administered and the responses received.

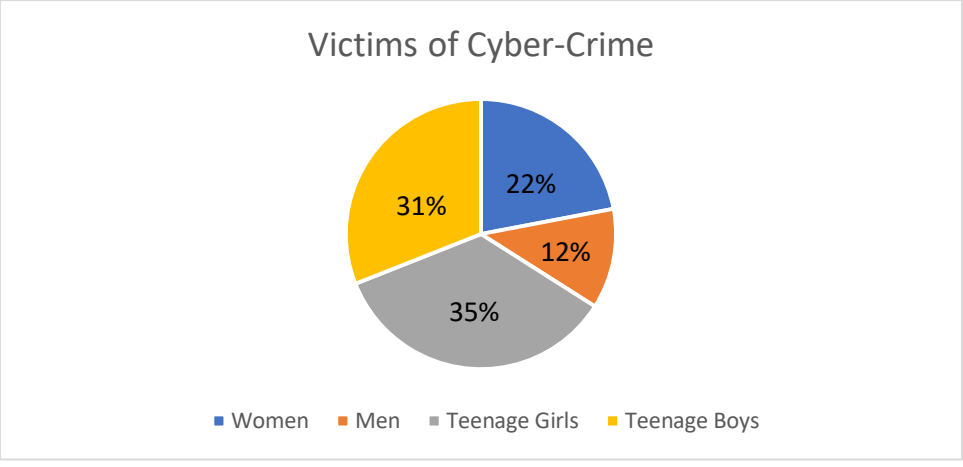
3.7.1. Sample Design :

4. **Cyber forensic Experts**
5. **Cyber Crime Investigating Officers**
6. **Group of 30 people**



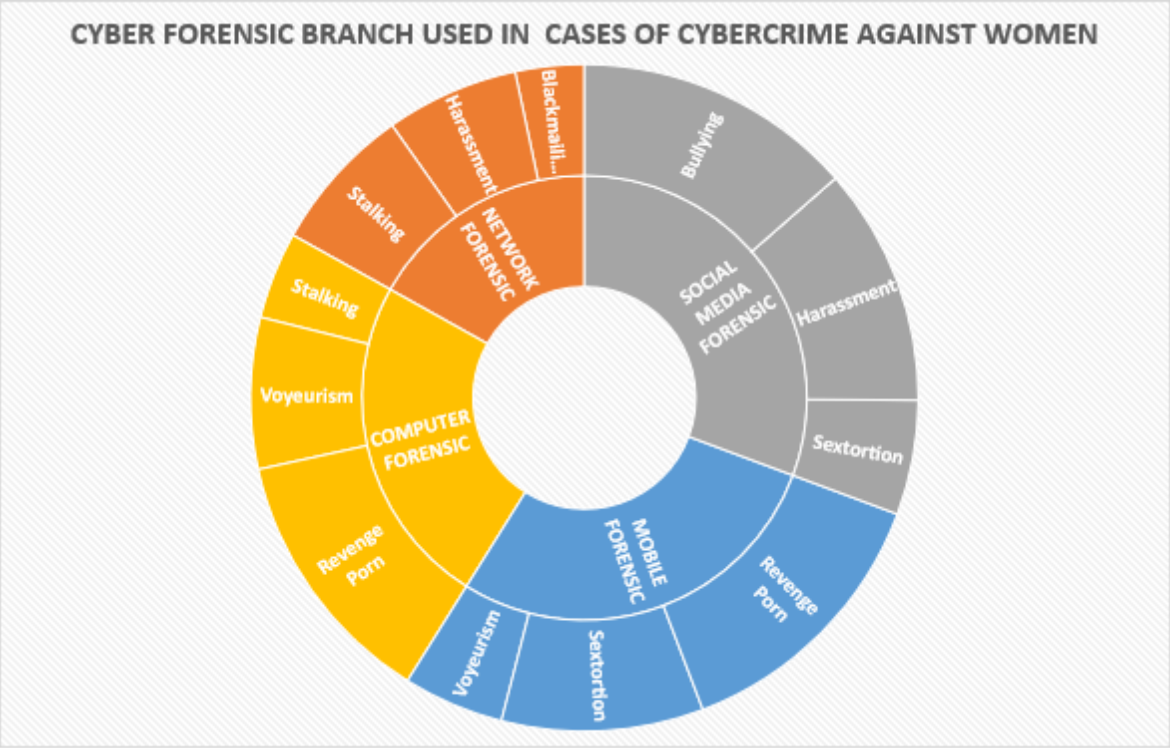
3.7.2. DETAILED ANALYSIS OF RESPONSES MADE TO EACH OF THE QUESTIONS IN THE QUESTIONNAIRE

1) Who are the most common victims of cyber-crimes in the digital space?



The survey results highlight that 35% of teenage girls are victims of various cybercrimes online, making them the most affected group. Teenage boys follow closely, with 31% falling victim to cybercrimes, ranking as the second-highest group targeted in the digital realm. In comparison, 22% of women experience cybercrime online, while only 12% of men are affected by similar offenses. Therefore, the survey finding shows that women and girls are disproportionately affected as victims compared to men. The data suggests that the prevalence of victimization among females is significantly higher, highlighting their increased vulnerability in the digital world. Teenage boys and girls are more prone to be targeted online as they are the easiest targets and are much active in the Internet and have less education on cyber safety. Teenagers are often the most vulnerable in the digital realm, as their natural curiosity leads them to explore new things online. However, this curiosity can sometimes make them hesitant to seek help or advice from elders or experts, leaving them open to exploitation and this lack of awareness and guidance around online risks exacerbates their vulnerability.

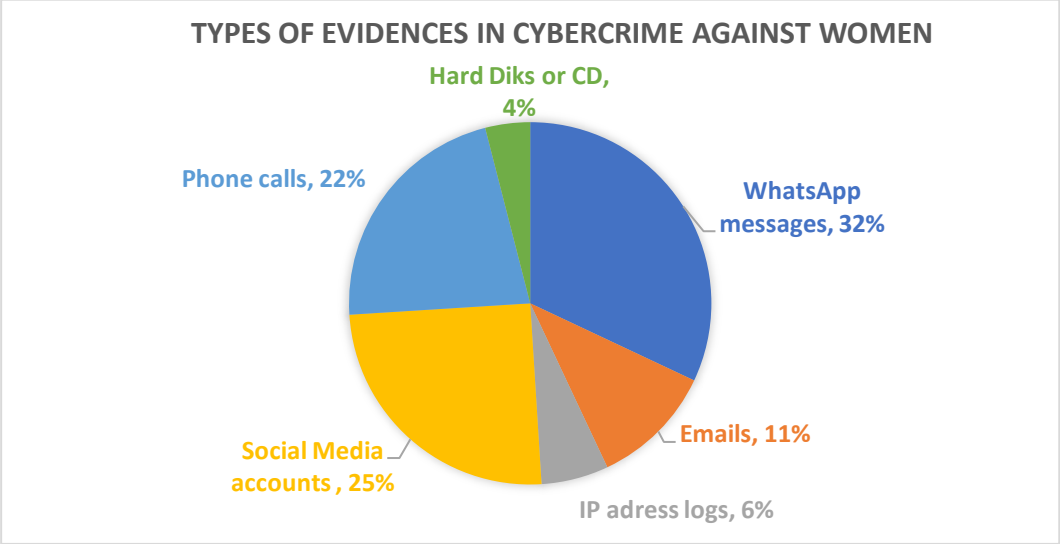
2) Which branch of Cyber Forensics is mainly used in cases of cyber-crimes against women?



Based on the survey, it has become evident that not all branch of cyber forensic is used in cases related to cybercrime against women. However, the mostly used branch of cyber forensics in the recent days are mobile forensic and network forensic. The above survey shows that four types of forensics are used in cases related to cybercrime against women. The first is **'Social Media Forensic'** where different social media cases such as 'bullying', 'harassment', and sextortion are dealt with. This branch of forensic is often used to remove any kind of obscene message or data or photo from the social media platform. The second is **'Mobile Forensic'** which deals to retrieve various data related to crimes such as 'Revenge Porn', 'Voyeurism' and Sextortion. The branch of Mobile forensic is also used to retrieve messages and data for the further investigation of the crime. The third is the **'computer forensic'** which is used in cases like 'voyeurism', 'stalking', 'revenge porn' etc. This branch is quite similar like the branch of mobile forensic. And lastly the most used branch of forensic used in cases of cyber-crime against women is 'network forensic' which deals with cases such as 'blackmailing', harassment' and stalking. This branch is used to identify the perpetrator by using special tools and techniques through the network system by tracking

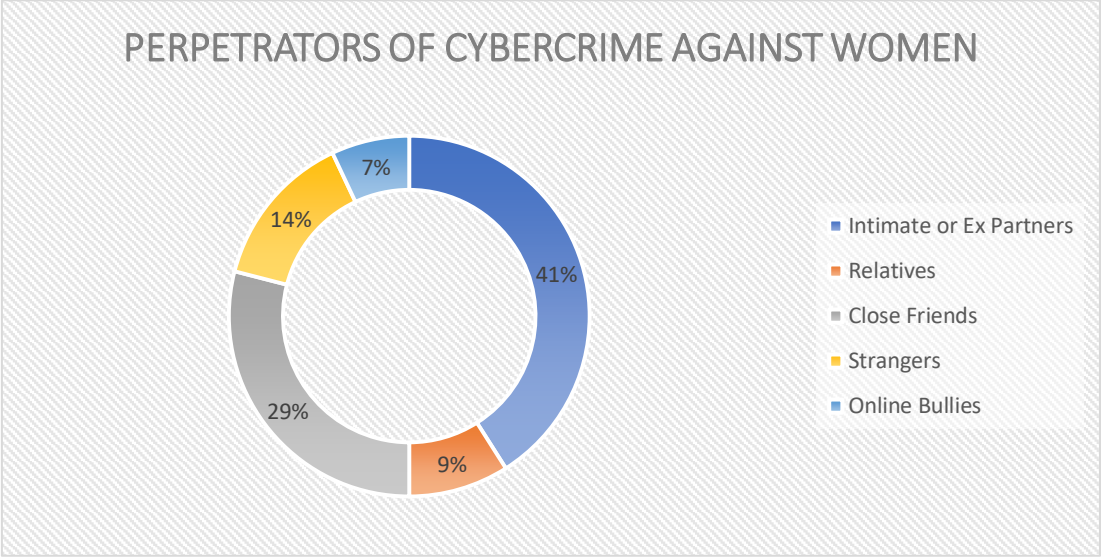
their IP address. Therefore, it is highlighted that though there are various branches of cyber forensics, these are the mostly common branch to deal with cyber-crime against women.

3) What are the different types of Evidences that are seen related to cybercrime against women?


TYPES OF EVIDENCES IN CYBERCRIME AGAINST WOMEN
Hard Diks or CD, 4%
Phone calls, 22%
WhatsApp messages, 32%
Emails, 11%
Social Media accounts , 25%
IP adress logs, 6%

The survey conducted among thirty forensic experts and investigators revealed that in cases of cybercrimes against women, the majority of the evidence typically comes from WhatsApp messages, phone calls, and other social networking platforms. Specifically, the data shows that 22% of the evidence is related to WhatsApp messages, 25% is from social media accounts, 22% from phone calls, 11% from emails, and 6% from IP address logs. It is evident that the most common types of evidence in cyber-crimes against women are WhatsApp messages and social media accounts, with perpetrators frequently using these platforms to target their victims. Phone calls, messages, and emails are commonly used by offenders to blackmail or threaten their victims. While IP address logs and hard disks are not as frequently cited as direct evidence, they are valuable tools in tracking the perpetrator's digital footprint and identifying their location or actions.

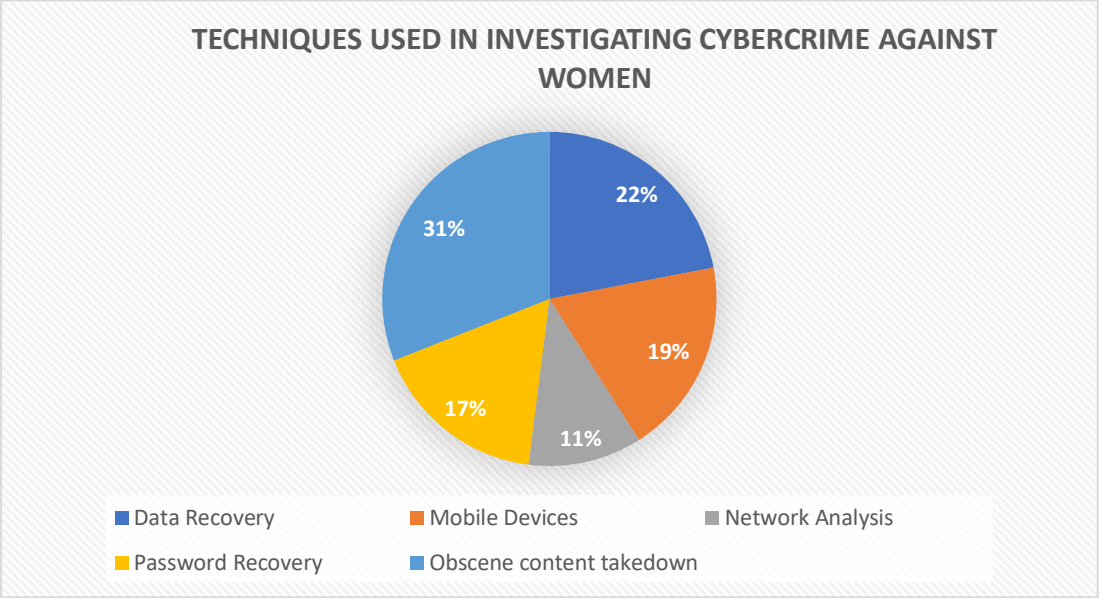
4) **Who are the most common types of perpetrators related to cyber-crimes against women?**



Based on the survey findings, it can be concluded that criminals frequently target women in cyberspace, primarily due to the anonymity the internet provides. This anonymity allows perpetrators to commit cybercrimes with reduced risk of immediate consequences. The data reveals that 41% of the perpetrators are intimate or ex-partners, 29% are close friends, 14% are strangers, 9% are relatives, and 7% are online bullies. It is particularly alarming that the majority of perpetrators are known to the victim. The largest group of offenders consists of intimate or ex-partners, who often engage in cybercrimes as a form of retaliation or revenge. This highlights the disturbing reality that many victims face threats and harassment from individuals they once trusted

.

5) **What are the different techniques used in investigating cyber-crimes against women?**



The survey findings revealed that certain investigative techniques are commonly used in cases of cybercrimes against women. These techniques include network analysis, data recovery, password recovery, and others. The data shows that 31% of investigations focus on obscene content takedowns, highlighting a troubling trend where victims are often sexually targeted, and explicit materials are used to blackmail them by being spread online. Additionally, 22% of the efforts are dedicated to data recovery, 19% to retrieving data from mobile devices, 17% to password recovery, and 11% to network analysis. These findings emphasize the critical role of digital forensics in combating cybercrimes and protecting the victims of such offenses. The mobile device and data recovery techniques are used to retrieve damaged data such as deleted photos, videos or messages. On the other hand, the technique of network analysis is used to track down the perpetrator and to track his actions and moves.

CHAPTER:- 4

CROSSING JURISDICTIONAL LINES: A COMPARATIVE LEGAL STUDY ON CYBER CRIME AGAINST WOMEN IN UK, USA, CANADA

4.1.Introduction

In the contemporary digital age, the increasing prevalence of cybercrime has emerged as a significant concern, particularly impacting women across various jurisdictions. Women around the world face disproportionate levels of online abuse, often targeting those from specific religious, ethnic, or racial backgrounds, sexual orientations, economic statuses, or those with disabilities. According to a 2017 Amnesty International poll, about one-quarter of the 4,000 women surveyed across the United States, United Kingdom, Denmark, Sweden, Spain, Italy, and Poland reported experiencing some form of online abuse, such as cyber harassment. Additionally, 41% of these women who encountered online abuse expressed fear for their personal safety as a result. Women have been subjected to intimidating messages, threats of violence, and sexually explicit communications through various online platforms, including dating sites, social media, chat rooms, and instant messaging services.[83] . The World Cyber Crime Index, revealed that the United States has a cybercrime threat score of 25.01, placing it in 4th position globally, while the United Kingdom ranks 8th.[84] The United States was the first country to witness the emergence of the Internet and also the first to experience internet-related crimes. In Europe, 18% of women, approximately 9 million, have faced some form of cyber violence since the age of 15. Among these, 7% have also encountered at least one instance of sexual or physical violence from an intimate partner.[85]

The cases related to cybercrime against women has experienced a hike in countries such as USA, UK and Canada. Sextortion and cyber harassment are the most prevalent types of cybercrimes affecting women.[86] The cybercrimes not only inflict emotional and psychological harms on the victims but also pose potential threats and challenges to law enforcement agencies and judicial systems across the globe. A report published by the council

[83] United Nations Office on Drugs and Crime, 'Gender-based interpersonal cybercrime' (2023) <https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html> accessed 10th June 2024

[84] Supra Note 3.

[85] UN Studies Association, 'Femicide: Volume XI, Cyber Crime Against Women and Girls' (2019) <https://www.unsavienna.org/sites/default/files/2020-01/FEMICIDE%20Volume%20XI.pdf> accessed 11th August,2024

[86] Ibid.

of Europe on Cyberviolence Against Women stated that 58% girls have faced online harassment of some sort among which 46% were misogynistic and sexist in nature.[87] If we look at the broader context, the global internet access report reveals that from 2019 to 2023 the number of male internet users increased by 7% while female internet users rose by only 3%.[88]Though the number of female internet users are less as compared to male users yet they are the most vulnerable ones to cybercrimes. As the digital realm of crimes is increasing protective measures are also being adopted in order to combat such crimes. The United Kingdom, the United States, and Canada, as leading democracies with advanced technological infrastructures, have developed comprehensive legal frameworks to combat cybercrimes. These nations have enacted legislations, established dedicated cybercrime units, and implemented various preventive and remedial measures to address the unique challenges posed by cybercrimes against women. Cyber forensics has played a significant role in these countries, with forensic experts utilizing various tools to combat cybercrime against women. The forensics departments in the UK, USA, and Canada are implementing measures through thorough investigations.

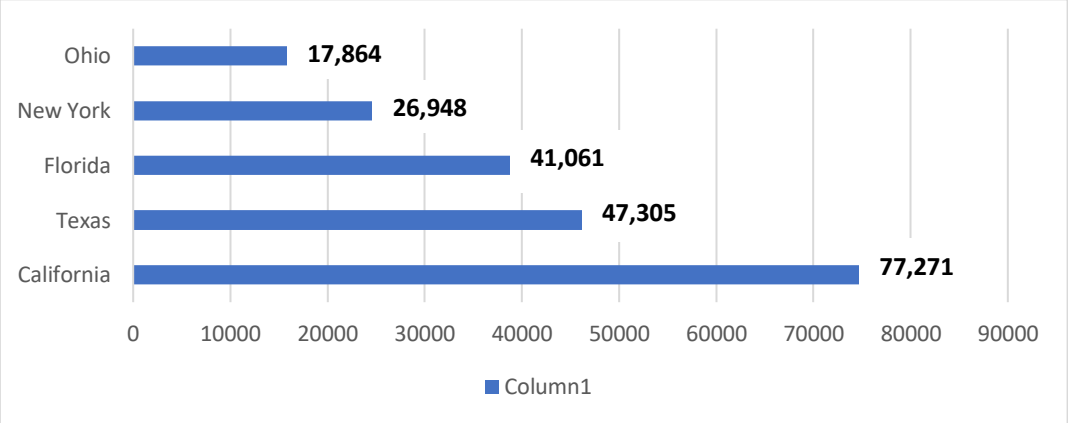
Initially, the data is recovered and extracted from remote systems and then those data are interpreted, often involving the synthesis of information from various sources and finally, those findings or the analysis are further presented in the court of law.[89] The concept of computer forensics was adopted by the FBI laboratory and other law enforcement agencies back at 1984 where they developed programmes to examine computer evidence.[90] The cyber forensics helps in extracting digital evidence which plays a vital role in, serving as the foundation for investigating and prosecuting cybercrimes. Proper handling of digital evidence is crucial to maintain its integrity for legal admissibility and despite all the challenges such as encryption and data volume, digital evidence often provides conclusive proof needed for

[87] Council of Europe, *Cyber Violence Against Women (2024),*
< https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women> accessed 10th June, 2024
[88] Global Digital Report, *Digital 2023-2019: Global Overview Report* <https://datareportal.com/reports> accessed 10th June 2024
[89] UK, House of Parliament, *Parliamentary Office of Science and Technology* <https://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf> accessed 12th June 2024
[90] Carrie Morgan Whitcomb, 'An historical perspective of Digital Evidence: A Forensic Scientist's View' (2002) 1 IJDE 25

legal outcomes.[91] Women are always found to be the most vulnerable one's related to cybercrime against women. It has become a significant concern worldwide.

4.2. Cyber Crime Against Women In USA

The United States has increasingly found itself at significant risk in matters related to cybercrime. As one of the world's most digitally connected nations, the U.S. is a prime target for cybercriminals, who exploit vulnerabilities in both government and private sector systems. According to the Federal Bureau of Investigation, the IC3 states that around 48,223 crimes were reported of Extortion, 55,851 crimes were reported of personal data breach.[92] The various types of cybercrime against women in the USA are Stalking, Harassment, Blackmailing, Cyber pornography and many more. Therefore, recognizing the specific vulnerabilities and challenges women face in digital space laws have been enacted to address cybercrime against women.[93] The internet crime report published by the Federal Bureau of Investigation, 2023 points out the most vulnerable states of USA that has reported maximum number of cybercrimes:[94]



According to the FBI's 2023 Internet Crime Report, the most common types of crimes reported against women include extortion, with 48,223 cases; identity theft, with 19,778 cases; and harassment or stalking, with 9,587 cases.[95] Several Federal Laws such as Violence Against Women Act, Communication Decency Act, Computer Fraud and Abuse Act

[91] U.S. Department of Homeland Security, 'Recommended Practice: Creating Cyber Forensics Plans for Control Systems' (2008) <https://www.cisa.gov/sites/default/files/recommended_practices/Forensics_RP.pdf> accessed 10th August, 2024

[92] Federal Bureau of Investigation, 'Internet Crime Report' (2023) <https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf > accessed 11th August, 2024

[93] Debarati Haldar, K. Jaishankar, 'Cybercrime and the Victimization of Women: Laws Rights and Regulations' (2011) IGI Global Publisher

[94] Supra Note 9

[95] Ibid.

addresses the various cyber offenses against women. The US laws have severe punishments and strong legislations to combat cybercrime against women, crimes such as Identity Theft, Online Sexual Exploitation, Cyber Stalking, Online Harassment imposes severe potential penalties to address this issue.[96]

The **Violence Against Women Act** is a legal framework that addressees different crimes against women. This is not a typical statute but is a part of broader legislation that encompasses various provisions across different titles and chapters. The Violence Against Women Act through its amendment in 2000 made cyber stalking a part of the federal interstate stalking statute and recognised it as a federal crime.[97] The **18 U.S. Code § 2261A** of federal law speaks about stalking which includes cyber stalking that states any person with an intention to harass, kill or intimidate another person uses the mail or any computer service or any electronic communication service commits an offence under this section. Cyber stalking is a major issue in the U.S where most of the stalkers are found to be men and the victims are found to be women. In the case of **United States v. Yung**,[98] Mr. Yung was rejected at an interview and therefore to take revenge, he created fake profiles to harass the interviewer's wife. He impersonated the woman and published an online ad seeking for a sex slave and as a result the victim got hundreds of phone calls seeking sex with the victim. This harassment turned the family's life into a nightmare and led them to emotional distress. The victim even received threatening messages through various electronic platforms. Eventually, the accused was charged with cyber stalking under 18 U.S.C. § 2261A(2)(B) & § 2261(b). The court ruled that his actions were clearly intended to cause significant emotional distress, which is a key element under this section and the conviction also highlighted the applicability of federal cyberstalking laws to cases involving persistent online harassment and threats. In another case of **United States v. Sayer,**[99] the defendant impersonated the victim, who was his ex-girlfriend by creating fake profiles on social media and dating apps. He posted the victim's personal information, including her home address and phone number, along with sexually explicit material, leading to strangers contacting and harassing her. Sayer was convicted of cyberstalking under the federal law of 18 U.S.C § 2261A. The court upheld his conviction, emphasizing that his actions constituted a clear pattern of harassment designed to cause significant emotional distress to the victim and gave

[96] Ibid.
[97] M.L. Pittaro, 'Cyber Stalking: An Analysis of Online Harassment and Intimidation' 1 IJCC 180 (2007)
[98] United States v Yung, 37 (3d Cir 2020)
[99] United States v Sayer, 748 (1st Cir 2014)

him 60 months of imprisonment. Cyberstalking is a crime that can affect anyone, regardless of gender; however, women are significantly more likely to be victims compared to men. Research shows that 1 in 10 women and 1 in 50 men have been stalked by an intimate partner, highlighting that women are more vulnerable to these crimes.[100]

Apart from Cyber Stalking, the second most common type of crime that are seen against women in USA are Sextortion and Sex trafficking. The FBI has reported a significant increase in sextortion cases over recent years, with thousands of cases reported annually. In 2022, the FBI received over 18,000 reports of sextortion.[101] Reports have shown that women are 1.17 times at greater risk of sextortion than men. During the pandemic, Native Alaskan and Indigenous North American women were 6.77 times more likely than White women to experience sextortion, while African American women faced a 7.33 times higher likelihood of experiencing sextortion compared to White women. Therefore, it was found that Native Black women are more likely to be victims of Sextortion.[102] There is no specific law directly addressing sextortion; however, it is covered under various federal laws. The **computer fraud and abuse act 18 U.S.C. § 1030** is often used in sextortion cases. This section criminalizes unauthorised access to computers which can be applied to several activities such as unauthorised access to obtain national defence, interstate foreign communications, government agencies, personal information of individuals etc.[103] The **18 U.S.C. § 2251** section criminalises Sexual Exploitation of Children which specifically address the production and distribution of child pornography. This statute is part of the broader framework of federal laws designed to protect minors from sexual abuse and exploitation.[104] The section **18 U.S.C. § 2422** which criminalises coercion and enticement of individuals to engage in illegal sexual activity. This statute is particularly concerned with protecting minors from sexual exploitation, as well as addressing attempts to persuade or coerce individuals into unlawful sexual acts.[105] In the case of **United States v. Moreira,** the defendant, Ricardo

[100] T.D. Robinson, 'Domestic Violence and Cyber Victimization: The Facts' College of Criminal Justice, Sam Houston State University, <https://dev.cjcenter.org/_files/cvi/October%202020%20Fact%20Sheet.pdf_1601995005.pdf>accessed 11th August, 2024

[101] Federal Bureau of Investigation, 'Internet Crime Report' (2022) <https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf > accessed 11th August, 2024

[102] Asia A. Eaton, Divya Ramjee and Jessica F. Saunders, *'The Relationship between Sextortion during COVID-19 and Pre-pandemic Intimate Partner Violence: A Large Study of Victimization among Diverse U.S. Men and Women'*(2022) < https://cybercivilrights.org/wp-content/uploads/2022/05/COVID-and-Sextortion-Eaton-2022.pdf>accessed 11th August, 2024

[103] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986)

[104] 18 U.S.C. § 2251 (2006)

[105] 18 U.S.C. § 2422 (2006)

Moreira, was sentenced to 30 years in prison for coercing numerous women and minors into producing sexually explicit images and videos by threatening to distribute previously obtained content. Moreira's actions were prosecuted under federal laws, including 18 U.S.C. § 2251 and 18 U.S.C. § 2422. The case demonstrates the use of federal laws against sexual exploitation and coercion in sextortion.[106]

Identity theft is a significant cybercrime affecting women in the USA. In 2021, approximately 23.9 million individuals fell victim to identity theft, with 9% of U.S. residents aged 16 or older being affected.[107] Females reported a higher number of identity theft cases compared to males and were more likely to experience identity theft over their lifetime.[108] Laws such as Identity Theft and Assumption Deterrence Act,1998, Identity Theft Enforcement and Restitution Act, 2008 penalises this crime. **The 18 U.S. Code § 1028** penalises Fraud and related activity in connection with identification, documents, authentication features and information. This section penalises identity theft and offenders convicted under this section are punished with an imprisonment of not more than 15 years.[109]

Other crimes against women such as revenge porn, cyber harassment are the most common types of crime that are committed against women in USA. Research shows that 83% of revenge porn victims had taken sexually explicit photos or videos of themselves and shared it with someone else, where 90% of women were found to be victims of revenge porn.[110] Revenge porn has been a concerning crime against women in the U.S. however, the federal law does not have any specific laws related to revenge porn and thus each state has approached to make their own laws to address this crime. States such as California, Florida, New York and Texas have come up with various legislations penalising revenge porn.[111]

The **California Penal Code Section 647(j)(4)** makes it illegal for anyone knowingly or intentionally distribute or disclose intimate images of another person without their consent. It specifically addresses situations where the intent is to cause distress or harm to the individual. The offender convicted under this section is penalised with an imprisonment up to six months

[106] United States v Moreira, 5 F Supp 3d 1290 (SD Fla 2014)
[107] Department of Justice USA, Bureau of Justice Statistics, *'Victims of Identity Theft'* (2023) <https://bjs.ojp.gov/library/publications/victims-identity-theft-2021> accessed 12th August,2024
[108] Ibid.
[109] 18 U.S. Code § 1028 (2009)
[110] Cyber Civil Rights (USA), *'End Revenge Porn, A Campaign'*(2022) < https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf>accessed 12th august,2024
[111] Z.J. Fernando, A.T Pase, 'Untangling the Tangle of Revenge Porn in the United States: A Comparative Study' 6 ICLR 77 (2024)

and/or fine up to one thousand dollars.[112]The **New York Penal Law under Section 250.45** criminalizes the distribution of intimate images without consent and also prohibits a person from recording or utilizing sexually explicit images of an individual.[113] This section was intended to protect individuals from having private images shared without their permission. However, the exact punishment of this offence can vary based on specific cases but generally in the punishment can extend from four to seven years of imprisonment.[114] The **Texas Penal Code** also criminalises the crime of Revenge Porn under **section 21.16** which speaks about unlawful disclosure or promotion of intimate visual material.[115] In Florida, The **Sexual Cyber harassment Act, of § 784.049** criminalises to disclose or threaten to disclose, an intimate image of another person without their consent.[116] The offender convicted under this section is punishable with an imprisonment up to one year. In the case of **Doe v. Google LLC**,[117] the plaintiff, referred to as Jane Doe, was an individual whose non-consensual intimate images were distributed online and the defendant, Google LLC, was sued because it hosted and indexed the intimate images, making them accessible through its search engine. In the case of **Patterson v. California,**[118] the defendant was charged under California Penal Code Section 647(j)(4) for unlawfully distributing the victim's intimate images without her consent, causing her significant emotional distress.[119]

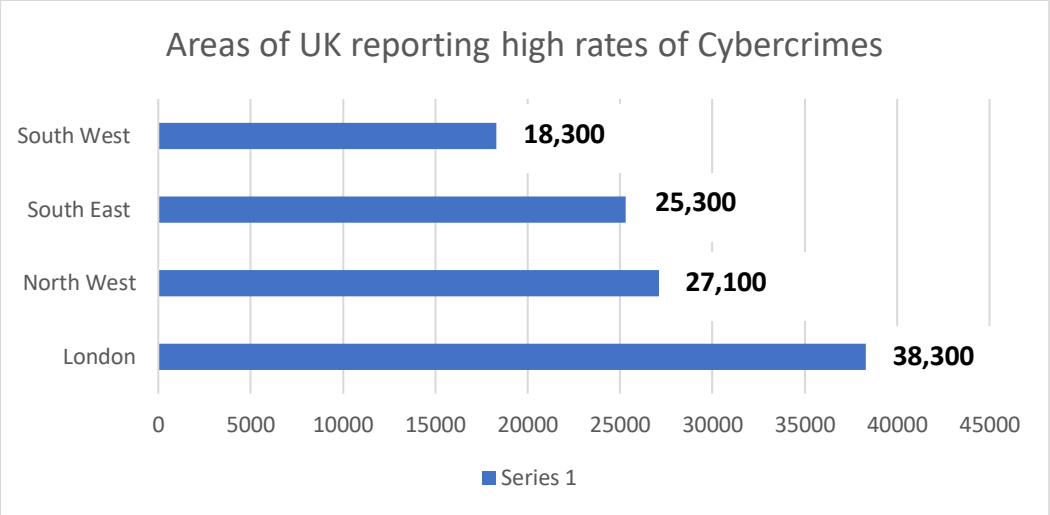
The landscape of cybercrime in the United States reveals a significant and growing threat, particularly impacting women. With high incidences of cyberstalking, sextortion, and identity theft, the need for robust legal mechanisms and effective enforcement is clear. Introduction of comprehensive federal laws, increased funding for victim assistance, encouraging cybersecurity measures and improved law enforcement training is required to address cybercrimes against women in USA.

4.3. Cyber Crime Against Women In UK

The United Kingdom has reported a growing threat of cybercrime cases against women, romance scams are the most prevalent type of crime affecting women in the UK. In 2021,

[112] California Penal Code, 1872 § 647(j)(4)i
[113] New York Penal Law, 1967 Section 250.45
[114] T. Cole, K. McGuffee, *'Freedom to post or invasion of privacy? Analysis of U.S. Revenge Porn State Statutes'* 20 IJERPP 1 (2020) < https://www.researchgate.net/publication/338953256.pdf> accessed 13th August,2024
[115] Texas Penal Code, 1973 Section 21.16
[116] The Sexual Cyber Harassment Act, 2015 Florida § 784.049
[117] *Doe v Google LLC* (2021) (ND Cal)
[118] Patterson v. California (2018) (ND Cal)

half of the romance scams victims were found to be women.[120] A 2023 report, from the UK Office for National Statistics indicated that women are more likely to experience online harassment than men. Approximately 23% of women aged 16 to 34 reported experiencing some form of online harassment.[121] In the UK, cases of online abuse have been notably prevalent among women, with one in five women reporting experiencing some form of online abuse.[122] The recognition of gender-sensitive cyber-crimes as a significant societal threat began in the UK only in the late 1990s, following widespread media coverage of stalking incidents involving female celebrities via the internet.[123] A report showing the analysis of cybercrimes reported from June 2022 to May 2023 pointed out the vulnerable areas of UK [124]



According to a report of EIGE, 2022 a survey conducted across 27 EU Member States including the United Kingdom found out that 11% of women had experienced cyber harassment since the age of 15.[125] In one survey, 41% of women in UK who experienced online abuse expressed concerns for their personal safety as a result of the abuse and harassment they faced.[126] The UK government also enacted various laws in order to control the threatening cybercrime against women focusing on online harassment, abuse, and exploitation.

---

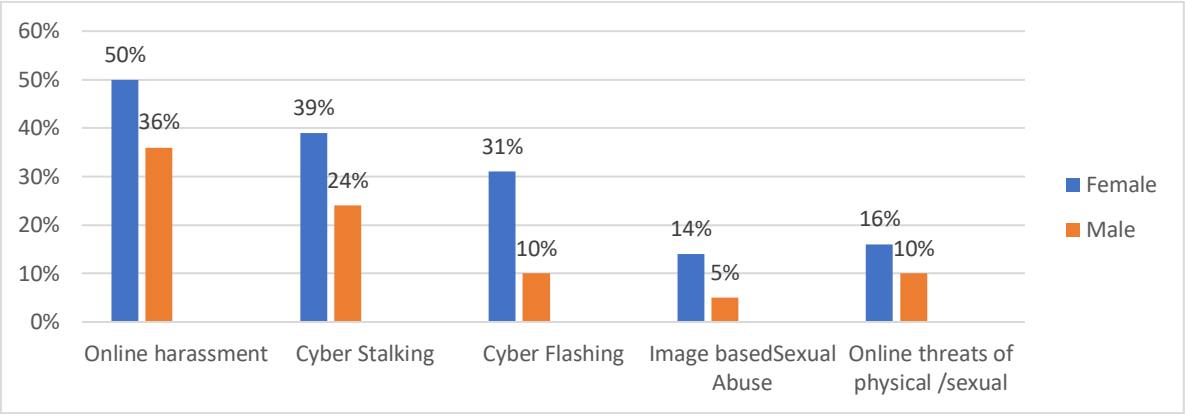
[120] Supra Note 2.
[121] Government of UK, Office of National Statistics, *'Experiences of harassment in 2023'* <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/experiencesofharassmentinenglandandwales/december2023> accessed 13th August, 2024
[122] Amnesty International UK, *'Online Abuse of Women widespread in UK'(2023) <https://www.amnesty.org.uk/online-abuse-women-widespread> accessed 13th August,2024*
[123] Supra Note 12
[124] Acora One, *'Latest Cyber Crime Statistics from the UK' (2024)* <https://acora.one/news/article/cyber-crime-statistics-uk> accessed 13th August,2024
[125] European Institute of Gender Equality, *'Combating Cyber Violence against Women and Girls' (2022)*
[126] UK aid, HM Government, 'Cybersecurity, Gender Equality & Social Inclusion' (2022)

The Computer Misuse Act, 1990 is the main legislation in the UK that addresses offenses involving attacks on computer systems. The Data Protection Act, 2018 from section 170-173 can also be used in cyber related offenses ensuring the protection of personal data from unauthorized disclosure.[127] Crimes such as cyber stalking and cyber harassment against women are penalised under the **Protection of Harassment Act, 1997** and **Malicious Communications Act, 1988. Section 1 and 2 of the Protection of Harassment Act, 1997** speaks about prohibition of harassment and offenders are penalised with an imprisonment of six months or with fine**.**[128] **Section 2A** of the Act, talks about stalking which penalises an offender of stalking through any means and prohibits behaviours like repeatedly contacting the victim online, monitoring their online activities, or publishing material about them. The offender convicted under this section becomes liable to imprisonment for a term not exceeding 51 weeks.[129] **The Communications Act, 2003 under Section 127** also penalises a person for the improper use of electronic communication used for sending offensive, obscene or indecent messages.[130]

The non-consensual sharing of intimate images or revenge porn in UK is a most frequent type of crime that are seen against women in the cyberspace. The UK revenge porn helpline in 2023, reveals that there has been a 106% increase in reports as compared to 2022. The UK revenge porn helpline had been combating intimate image abuse since 2015 and it has removed over 305,000 images across online platforms in 2023.[131] According to police data, 3520 cases of revenge porn were reported in the UK between 2019 and 2022, and 2780 of those victims were female. However, only 87 cases resulted in charges or summons being issued, while the remaining cases remained pending due to evidentiary difficulties.[132] Revenge Porn in UK is primarily addressed under the **Criminal Justice and Courts Act, 2015 under Section 33** which prohibits disclosure of private sexual photographs and films with an intent to cause distress and a person convicted under this section is punished with a term of imprisonment for two years.[133] The **Data Protection Act, 2018 from Section 170 –**

[127] Government of UK, Crown Prosecution Service, 'Cybercrime Prosecution Guidance' (2024) <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>accessed> 13th August, 2024
[128] Protection of Harassment Act, 1997, Section 1 & Section 2
[129] Protection of Harassment Act, 1997, Section 2A
[130] The Communications Act, 2003, Section 127
[131] UK Safer Internet Centre, Revenge Porn Helpline, 'The Revenge Porn helpline reveals 106% increase in reports' (2024) < https://saferinternet.org.uk/blog/the-revenge-porn-helpline-reveals-106-increase-in-reports>accessed 13th August,2024
[132] Metropolitan Police UK*, 'Data on Revenge Porn from January 2019 to July 2022' (2022)* <https://www.met.police.uk>accessed 14th August, 2024
[133] Criminal Justice and Courts Act, 2015, Section 33

173 discusses about the offenses relating to the misuse of personal data and protects from the unlawful obtaining or disclosure of personal data. Apart from these laws, the Online safety Act, 2023 is a significant piece of legislation in the UK aimed at regulating online platforms and protecting users, particularly against harmful content.[134] **Section 187 and 188 of the Online Safety Act, 2023** intends to prevent revenge porn, which speaks about y criminalizing the act of sending or threatening to send obscene images. Offenders may face up to two years of imprisonment and a fine.[135] Other crimes such as online sexual abuse, sextortion, online impersonation are also seen against women. However, according to a survey conducted in the United Kingdom in 2022, the most common type of online crimes are cyber bullying, online harassment and cyber stalking.[136] A survey conducted in 2022 pointed out the most prevalent types of cybercrime committed against women as compared to men in the UK:[137]



Cyber flashing is a type of crime that is most prevalent against women in UK which refers to the unsolicited sending of sexually explicit images or videos through digital platforms without the recipient's consent. A research conducted by Professor Jessica Ringrose in 2020 found that 76 percent of girls aged 12 to 18 years has been victim of cyber flashing.[138] The United Kingdom recognising the seriousness of this crime, made it a criminal offense under **Section 187 of the Online Safety Act, 2023** which penalises *'sending photograph or film of*

[134] Data Protection Act, 2018, Section 170-173
[135] South Wales Police, Gov. of UK, 'New Law make it illegal to share picture or films of personal nature without consent' (2024) < https://www.south-wales.police.uk/news/south-wales/news/2024/march/online-safety-act-2023/>accessed 14th August, 2024
[136] Statista, *'Types of online abuse experienced by victims in the United Kingdom as of February 2022',* <https://www.statista.com/statistics/1319815/uk-online-abuse-experienced/>accessed 14th August, 2024
[137] Ibid.
[138] Government of UK, 'Cyberflashing to become a criminal offense' (2022) <https://www.gov.uk/government/news/cyberflashing-to-become-a-criminal-offence>accessed 14th August,2024

genitals' and a person convicted of this crime is subjected to an imprisonment for a term of two years.[139]

The United Kingdom has enacted robust legal frameworks and measures in order to control cybercrimes against women. The UK's approach demonstrates a commitment to addressing the complexities of cybercrime and safeguarding the rights and safety of women online. Cybercrime research in UK is more focused on analysing and drafting legislation that addresses cybercrimes related to national security, financial stability, corporate identity and information protection, and child safety. The UK takes a more conservative approach in regulating gender-centric cyber harassment, particularly in cases that do not involve physical harm. By incorporating offenses related to non-consensual sharing of intimate images, harassment, and stalking, the legal system acknowledges the severe impact of these crimes have on victims. To tackle different crimes such as revenge porn, sextortion and online sexual abuse various measures are taken by the government to address the issue immediately so that it does not affect the victim any further. The collaborative approach of UK with global organizations, such as Interpol and Europol, strengthens cross-border cooperation and collaborative approach enhances the country's international cybersecurity efforts. The UK's law enforcement agencies, including the National Crime Agency (NCA) and the Cyber Crime Unit, play a pivotal role in combating cybercrime. The United Kingdom has focused on the adaptation of new laws such as Online Safety Act, Data Protection Act and Communications Act to address the emerging threats in the cyberspace. The UK's legislative framework sets an important precedent for other jurisdictions and highlights the necessity to adapt new laws with the evolving technology.

4.4. Cyber Crime Against Women In CANADA

Like many other countries, Canada also continues to report highest cases of cybercrimes against women. Women in Canada often fall victims of cybercrime, data reveals 1 in every 5 women reports a case of cyber harassment in Canada. Among which 30% of them reports unwanted behaviour online and 44% of women become targets of online hate speech.[140] Canada is increasingly reporting highest cases of cybercrime since the past years, there has been 93,068 police reported cases in Canada relating to cybercrime which saw a rise of

[139] Online safety Act, 2023, Section 187

[140] Canadian Women's Foundation, *'Gendered Digital Hate, Harassment and Violence'* (2024) <https://canadianwomen.org/> accessed 14th August, 2024

15.98%.[141] There are different types of crimes that women most commonly face under the digital realm such as cyberbullying, digital hate, online sexual violence and harassment.[142] In Canada, the legal framework has been evolving to address these challenges, with laws such as the Criminal Code and the Protecting Canadians from Online Crime Act aiming to provide protection and justice for victims.

Cyber bullying is a serious crime that is committed in the cyberspace and can have negative impact on the individuals. In Canada, cyber bullying is one of the prevalent crimes that are committed in the digital realm, 3 out of 10 youth in Canada say that they have been victims of cyber bullying.[143] Cyberbullying is prevalent in Canada both amongst males and females equally, however data shows that 24% of males and 25% of females experience some sort of cyber bullying. [144] **The Criminal Code of Canada** does not have a specific provision related to cyber bullying but provisions such as **Section 264** which speaks about criminal harassment penalises a person if they intentionally engage in a behaviour which leads another person to reasonably fear for their own safety. This crime is subjected to an imprisonment up to ten years. The Protecting Canadians from Online Act which received its royal assent on December 9, 2014 also amended the criminal code of Canada to address the issues of cyber bullying and other online crimes. [145] Cyber sexual harassment is a growing issue amongst women in Canada. A survey was conducted among women across Canadian universities where it was found 58% of them reported gender-based hate speech, 53% reported instances of sexual harassment and 52% of them reported experiences of non-consensual pornography.[146] Non consensual pornography and online sexual harassment is widely experienced by women in the cyberspace in Canada. **Section 163 of the Criminal Code of Canada** deals with offenses related to the publication, distribution, and possession of obscene materials and an individual found guilty under this section may face imprisonment, fines, or both.[147] **Section 162** of the Canadian Criminal Code, penalises the offence of voyeurism and

[141] Statista, Canada Police Reported cybercrime instances 2023, <https://www.statista.com/statistics>accessed 14th August,2024
[142] Supra note 61
[143] Government of Canada, 'What is Cyberbullying' (2024) <https://www.canada.ca/en/public-safety-canada/campaigns/cyberbullying.html>accessed 14th August, 2024
[144] Darcy Hango, 'Online harms faced by youth and young adults: The prevalence and nature of cyber victimization'(2023) <https://www150.statcan.gc.ca/n1/pub/75-006-x/2023001/article/00003-eng.htm>accessed 14th August, 2024
[145] Parliament of Canada, 'Statutes of Canada, 2014' Chapter 31 <https://www.parl.ca/DocumentViewer/en/41-2/bill/C-13/royal-assent>accessed 14th August, 2024
[146] Jenna Cripps, Lana Stermac, 'Cyber Sexual Violence and Negative Emotional States among women in a Canadian University' 12 IJCC 171 (2018)
[147] Criminal Code of Canada, 1892, Section 163

a person found guilty of this offence is punished with an imprisonment of maximum five years.[148] The offense of Identity Theft is also penalised under Section 402 of Criminal Code of Canada which states that a person is guilty of an offense if they acquire or possess someone else's identity information with the intention of using it to commit an indictable offense that involves fraud, deceit, or falsehood.[149] Though the criminal code of Canada contains specific provisions to control various cybercrimes against woman, yet the **Personal Information Protection and Electronic Documents Act** is a federal privacy law in Canada that focuses to set rules for the collection, use, and disclosure of personal information in a technology-driven era, balancing individuals' privacy rights.[150] This act is Canada's national private sector data privacy law, which is primarily designed to protect digital data by regulating private sector organizations that collect or share personal information in the course of their commercial activities.

Canada's approach to cybercrime against women differs notably from both the US and the UK. Canada follows the British Penal system for both offline and online crimes and its socio-legal approach to cybercrime is more aligned with the US yet it does not have any gender-specific legislation. However, the governmental efforts to spread awareness through police handbooks are notable in regards to cyber-crimes against women. A significant challenge in Canada is the absence of comprehensive statistical data on the victimization of women in cyberspace, making it difficult to analyse trends from a quantitative perspective.[151] Though Canada laws focus on various cyber offenses yet the women's victim's rights are not addressed. Cybercrime is not gender specific yet data and surveys shows that women report highest cases of cyber victimisation. Canada needs to focus on harsh punishments and gender specific regulations in order to control the harassment of women beneath the cyberspace.

4.5. International Conventions For Cybercrime Against Women

To control the rate of cybercrime against women in the cyberspace is dealt with different perspectives by different countries. Like the USA, many countries do not have gender specific laws to fight the growing threat of cyber victimisation against women. Women in the cyberspace are getting victimised by the perpetrators and we need a specific gender-based

[148] Ibid. Section 162
[149] Ibid. Section 402
[150] Personal Information Protection and Electronic Documents Act, 2000 <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html#h-416931>accessed 14th August, 2024
[151] Supra note 13, chapter 6

law to fight this. There are certain international conventions that had actually focused in controlling and combatting the cyber victimisation of women.

4.5.1. The Istanbul Convention: This convention is also known as the **Council of Europe Convention preventing violence against women and domestic violence** which was adopted by the Committee of Ministers of the Council of Europe on 7th April, 2011 and entered into force on 1st August, 2014 and as of 2021, is the first convention in Europe which focused specifically to control gender-based violence. This convention has 39 states, as of 2024 who are parties to the treaty and stands as a landmark treaty for women's rights offering the most extensive measures for governments to prevent and address all forms of violence against women including domestic violence and frames such violence as a violation of human rights and a discrimination against women.[152] Though this convention do not have any specific provision regarding the digital dimension of violence against women but it's scope mentioned in **Article 2** of the convention states *'this act applies to all forms of violence against women, including domestic but particular attention should be paid to women'* shows that it includes violence against women in the digital space, as intended by the drafters. **Article 34** of this convention speaks about 'stalking' which criminalises repeatedly engaging in threatening activity in order to cause fear to somebody.[153] Given the severe psychological impact that various forms of online and technology-facilitated violence can have on women and girls which causes emotional distress to them, the Istanbul Convention's obligation to criminalize psychological violence under **Article 33** becomes particularly significant. The provision of **Article 40** can also be applied to the online sexual harassment which states that '*any form of unwanted verbal or non-verbal conduct of sexual nature intended to violate a person's dignity is subjected to leal penalties.'*[154] The Istanbul convention though do not specify any specific provision relating to online victimisation of women, yet the drafters of the convention stated that the crime of stalking also includes following the victim in the cyberspace.[155] Though the Istanbul convention have framed a specific legislation focusing on the crimes against women, yet they did not recognise the growing threat against women in the

[152] Council of Europe, A. Wilk, *'Protecting Women and Girls from Violence in Digital Age: The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women'* (2021)
[153] Ibid.
[154] Ibid.
[155] Gizem Guney, 'The Istanbul Convention: A Missed Opportunity in Mainstreaming Cyberviolence against Women in Human Rights Law?' (2022) EJIL <https://www.ejiltalk.org/ >accessed 14th August, 2024

virtual world which encompasses a wide array of crimes against women such as deepfakes, cyberbullying, revenge porn, sextortion etc.

The convention is regulated through GREVIO which an independent body comprising of 15 members and conducts country by country evaluation ensuring the effective application of the framework to prevent the violence against women. Though, the Istanbul convention has focused on the gender specific laws is order to control the various forms of violence against women, yet they have failed to mention specific framework regarding cyber violence of women. However, the scope of the framework covers all forms of violence against women, yet serious technology facilitated crimes against women such as revenge porn, sextortion and other types of online crimes should have been addressed which is the need of the hour.

4.5.2. The Budapest Convention: The Budapest Convention is called the **Council of Europe Convention on Cybercrime** and is the first legally binding treaty protecting cyber related offenses. This convention was adopted on 2001 and came into force on 1st July 2004 having 76 signatories as of 2024.[156] This treaty was adopted in order to control the growing threat of cybercrime. **Article 2 and 3** of the convention criminalises illegal access and interception that criminalises unauthorised access to computer systems and unauthorised transmission of computer data that can include a woman's private information or accounts.[157] **Article 10** of the convention speaks about offenses related to child pornography which can affect young girls. The Budapest convention doesn't contain provisions focusing particularly against women yet it provides a valuable framework for considering the issue of online violence against women, particularly in connection with the Istanbul Convention. Through various substantive criminal law provisions, the Budapest Convention directly and indirectly addresses certain forms of online and technology-facilitated violence against women.[158]

Therefore, the Budapest convention offers a very interesting framework to control the different facets of cybercrime but it has focused on cyber related issues on a general sense and does not contain any gender-specific provision. While it does not explicitly focus on gender-based violence, its provisions can be applied to combat various forms of cybercrime that target women. The growing threats of different violence against women in the cyberspace requires a robust legal framework to tackle it. Almost every other country all over the world

[156] Council of Europe, 'The Convention on Cybercrime' <https://www.coe.int/en/web/cybercrime/the-budapest-convention>accessed 14th August, 2024
[157] Council of Europe, Convention on cybercrime (2001) accessed 15th August, 2024
[158] Supra Note 72

face some sort of serious cyber violence against women and therefore to tackle this issue we need to develop certain gender-specific provisions controlling violence of women in the cyberspace.

4.6. Admissibility Of Digital Evidence:

United States of America (USA):

The admissibility of digital evidence depends on various factors such as relevance, authenticity, best evidence rule, chain of custody etc. Digital Evidence in the US is governed by a combination of federal and state rules of evidence, judicial precedents ad statutory laws. The **Rule 401 of Federal Rule of Evidence** states that for digital evidence being admissible in court, it must be relevant. This typically involves showing that the digital evidence has not been altered and that it originated from a reliable source.[159] The **section 901 of federal rule of evidence** states that digital evidence must be authenticated and imposes high standards of collection and analysis of digital evidence. The establishment of the authenticity often requires testimony by forensic experts which is laid down in Rule 702.[160] The admissibility of digital evidence is also dependent on the 'best evidence rule' from the federal rule of evidence section 1001 to 1004 which states that the Best Evidence Rule requires that to prove the content of a writing, recording, or photograph and the original evidence must be produced. In the context of digital evidence, "original" can include any printout or output that accurately reflects the data. Duplicates or copies of digital evidence are generally admissible unless a genuine question is raised about the original's authenticity or if admitting the duplicate would be unfair.[161] In the famous case of **Commonwealth v. Markoff** [162], also known as the *'Craigslist Killer'* case the accused committed an offence of robbery, murder and assault of a woman. The victims were constantly in touch with the accused through emails and when the investigators traced the emails, they found an IP address which led them to the accused, a 23year old medical student Phillip Markoff. This case led the landmark victory of digital forensics and the digital evidences were provided in court as a proof. Thus, the landscape of digital forensic is an ever-evolving area in combatting not only cybercrimes but also tracing offenders who are out of the reach.

[159] G.W Manes, 'New Federal Rules and Digital Evidence' (Conference on Digital Forensics security and law, 2007)
[160] Ibid.
[161] Ibid.
[162] Commonwealth v. Markoff, No. SUCR2009-10614 (Mass. Sup. Ct. 2009)

United Kingdom(UK):

In the UK, the admissibility and handling of digital evidences is governed by various acts such as the **Police and Criminal Evidence Act, 1984 Section 69** which speaks about the admissibility of computer records. This section was repealed in 2000, which established that computer evidence is considered reliable unless proven otherwise.[163] The Electronic Communications Act, 2000 under Section 7 give recognition to electronic signature, data and communications shall be admissible and presented in court.[164] Section 3 of the Computer Misuse Act 1990 outlines a list of unauthorized acts related to a computer with an intent to impair or cause recklessness to the operation of the computer and penalises the person found guilty of such offense. In the case of **Grant v. Southwestern and County Properties Ltd**, the Supreme Court of the UK stated that tape recording qualifies as a valid document as it meets all the necessary criteria and essential elements associated with it. Also, in the **17th session in 1984, the UNCITRAL** spoke about the legal aspects of automatic data processing and **Article 5** of the model law gave legal recognition to data messages which stated that information presented as data messages cannot be rejected solely because it is in electronic form.[165] The admissibility of digital evidence in the UK courts is governed by a combination of statutory provisions, case law, and procedural rules. Ensuring that digital evidence is authentic, relevant, and fair involves rigorous standards of testing its authenticity and maintaining a proper chain of custody. The legal system continues to adapt to technological advancements, striving to balance the need for effective prosecution and protection of individual rights.

Canada:

In the Canadian legislation, the admissibility of digital evidence is governed by a combination of various statutory provisions and common law principles. **Section 31.1 of the Canada Evidence Act**, speaks about the authenticity of digital evidence and states that any person seeking to admit electronic evidence must also demonstrate it's authenticity. **Section 31.2** speaks about the application of best evidence rule in cases of electronic documents. **Section 31.3** talks about the integrity of an electronic evidence stating that the evidence must show that the computer system or similar device used to record or store the document was

[163] Chris Reed, 'The Admissibility and Authentication of Computer Evidence - A Confusion of Issue' (5th British and Irish Legal Technology Association conference, 2005)
[164] Electronic Communications Act, Section 7
[165] D. Goswami, H. Bahaduria, 'Admissibility of electronic evidence in the courts of India and United Kingdom: A detailed analysis' 6 IJL 83 (2020)

functioning properly at all relevant times, or if it was malfunctioning, it did not affect the document's integrity and there are no other reasons to doubt the system's reliability.[166] Though certain forms of electronic evidence is admissible in the court, however social media evidence is inadmissible in the courts of Canada and an electronic document to be admissible in Canada the party must establish authentication and presume the integrity.[167] In the case of **R v. Ghomeshi**,[168] This high-profile case involved Jian Ghomeshi, a former CBC radio host accused of sexual assault of two woman. Digital evidence, including social media messages and email communications, played a significant role. The case highlighted the importance of digital communications in corroborating or disputing allegations.

In the case of **R. *v.* Jarvis**,[169] the accused was charged with an offence of voyeurism of women under S. 162(1)(c) of the Criminal Code of Canada and as an evidence 35 video files were recovered from his phone and those evidence were brought in front of court under Section 32 of the Canada Evidence Act and a proper chain of custody was followed for the admissibility of the evidence. Therefore, digital evidence played a very important role in this case. Canada has specific legislations for the admissibility of digital evidence in the court and depending on the authenticity, reliability and the chain of custody these evidences are admissible in court.

CHAPTER:- 5

SAFEGUARDING WOMEN: THE JUDICIARY'S ROLE IN COMBATTING CYBER CRIME AGAINST WOMEN IN INDIA.

In India, the judicial system acts as a guardian of justice and plays a vital role in curbing different crimes across the country including cybercrimes against women. It achieves this by providing legal remedies, setting judicial precedents, and ensuring the effective implementation of laws. The Supreme Court, in particular, interprets constitutional provisions and existing legislation authoritatively to combat online violence against women. With the rise of various online platforms, the need to tackle cybercrime has become more pressing

[166] Criminal Evidence Act, 1985 Section 31.1- 31.3
[167] W.K. Gorman, 'The admissibility of social media evidence in Canada part 2: The Canada Evidence Act'(2021) The Journal of the American Judges Association
[168] R v Ghomeshi [2016] ONSC 7671
[169] R. *v.* Jarvis, 2019 SCC 10, [2019] 1 S.C.R. 488

than ever. India has witnessed a significant surge in cyber threats. According to the Indian Cyber Crime Coordination Centre (I4C), a total of 740,000 cybercrime cases were reported in the first four months of 2024 alone.[170] Furthermore, projections indicate that India could experience up to 1 trillion cyber-attacks annually by 2033 which can escalate till 17 trillion by 2047.[171] Today the technology has been rapidly increasing with time and it has also brought innovative changes in the judicial system. The integration of digital tools, artificial intelligence and data protection bills, has revolutionised the justice delivery system related to cybercrime cases. These innovations aim to enhance the judicial system's efficiency, transparency, and accessibility while also presenting with new challenges.[172]

Technology not only has the power to connect people, but also the power to reinforce and disseminate social and cultural structures and helps normalize gender roles but it has dark side also and strongly impact on our lives as well. In 21st century Cybercrimes the new form of crimes and which are most challenging crimes to curb it. It is more challenging in India as legal awareness regarding cybercrime is very poor. Gender based violence at cyber space some like Cyber harassment, Cyber stalking, Cyber pornography, Cyber defamation, Morphing, Email Spoofing etc. have been increasing due to digital revolution. In the era of digital revolution Women and children have been softly targeted and victimised easily at cyber space. The changing nature of the society increases the role of the adjudicatory authority in the present days. In the era of Information and technology, the criminals are using new technology to commit the crime. [173]

Therefore, appropriate judicial approach towards the technological offences is required for prevention of the crime. For the proper working of the judiciary the rules of jurisdiction plays an important role. Effective legal machinery can be identified on how properly rules and regulations are drafted by legislation and more importantly how precisely principles of jurisdiction are laid down. A court must have jurisdiction, venue and appropriate service of process in order to hear a case and render an effective judgment.5 So Judiciary has been playing crucial role to protect the rights of women. This research paper is giving brief view about cybercrimes against women and cyber law along with the role of judiciary in today's

[170] Ministry of Home Affairs, Indian Cybercrime Co-ordination Centre (I4C) (2024) < https://i4c.mha.gov.in/> accessed 11th January, 2025

[171][171] Central Reserve Police Force, 'Cyber Attacks on India- Cyber Byte.pdf' (2024) <www.crpf.in>accessed 12th January, 2025

[172] Neha K. Bhatt, *'A Challenging Role of Indian Judiciary at Cyber Space to curb Cybercrime against Women'* (2021) 4 GJIS 41

[173] Priya Gupta, *'Cyber Crime Against Women in Indian Context: An Overview'* (2020) 8 JRHSS 75

context the new form of crimes against women at cyber space which need to be combat effectively. There are so many definition which given by different author. In common parlance Cybercrime or Computer oriented crime," is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.[174]

5.1. Legal Frameworks Protecting Women

Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. In India the term "Cybercrime against women" includes sexual crimes and sexual abuses on the internet. India is among the very few countries to enact Information Technology Act, 2000 to combat cybercrimes. This Act widely covers the commercial and economic crimes which are clear from the preamble of the Information Technology Act, 2000. The act deal with legal recognition of electronic documents and digital signatures, Offenses and contraventions and justice Dispensation Systems for cybercrime. The key sections of the Information Technology Act which deals with cybercrime against women are:[175]

- **Section 66A:** This section deals with the provision relating to the **punishment for sending offensive messages through communication service**. This states that if any person sends a grossly offensive or menacing message or character with a purpose to cause inconvenience, danger, and criminal intimidation shall be punished with an imprisonment for three years and with fine.
- **Section 66C:** This section states the **punishment for identity theft** which states anyone who fraudulently or dishonestly makes use of any unique identification feature of any other person shall be punished with an imprisonment which may extend up to three years and with a fine which may extend to one lakh rupees.
- **Section 66D:** This section speaks about the **punishment for cheating by personation by using computer resource**. It states that through any communication device or computer resource if any person cheats by personation shall be liable to an imprisonment for three years and with a fine up to one lakh rupees.
- **Section 66E:** This section specifies the **punishment for violation of privacy** which states that anyone who knowingly transmits or publishes any image of a private area

[174] Ibid.
[175] *Information Technology Act,* 2000 (India)

of any person without his or her consent and violates the privacy of that person shall be liable with an imprisonment which may extend up to three years or with a fine not exceeding two lakh rupees.

- **Section 67:** This section addresses with the **punishment for publishing or transmitting obscene material in any electronic form** which says that whoever publishes or transmits any obscene material shall be punished with an imprisonment of three years and a fine of five lakh rupees in first conviction and in case of second conviction, the punishment increases with an imprisonment of five years and a fine of ten lakh rupees.
- **Section 67A:** This section deals with the **punishment for publishing or transmitting sexually explicit content in any electronic form**. The section states any person who publishes or transmits any sexually explicit content shall be punished with an imprisonment of five years and a fine of ten lakh rupees in first conviction and in case of second conviction, the punishment increases with an imprisonment of seven years and a fine of ten lakh rupees.

Previously, the Information Technology Act had certain loopholes that needed to be addressed. After careful discussions with various advisory groups and bodies, a major amendment was made in 2008, which came into force on **27th October 2009**. This amendment introduced **Sections 66A to 66F**, which expanded the scope of offenses and penalties related to cybercrimes. Additionally, the amendment increased the term of imprisonment and the fine stipulated in **Section 67**. It also introduced **Section 69**, granting authorities the power to carry out the "interception, monitoring, or decryption of any information through any computer resource."[176]

The **Indian Penal Code, 1860** also criminalizes various cybercrimes targeting women, and the investigation process has consistently relied on this code to ensure proper handling of such cases. This code criminalises several offenses and while the IPC does not specifically focus on "cybercrimes," several sections of the IPC are applicable to offenses that occur in the digital space, particularly those that target women.[177]

- **Section 292:** This section speaks about **'Sale, etc., of obscene books, etc'** which says that any person who prints, sales or advertises any obscene picture or object shall be

[176] Akansha Pathak, *'Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws'* (2013) 59 NLUJAA 64
[177] Indian Penal Code, 1860 (India)

punished with an imprisonment for a term of two years and with a fine of two thousand rupees in case of first conviction and in case of second conviction it may extend to five years and five thousand rupees.

- **Section 354:** This section speaks about **Assault or criminal force to woman with intent to outrage her modesty** which specifies that any person by use of criminal force intending to outrage a woman's modesty shall be punished with imprisonment which shall not be less than one year but which may extend to five years, and shall also be liable to fine.
- **Section 354A:** This section deals with **sexual harassment and it's punishment** which says that any person making physical contact involving any sexual gestures, or asks for sexual favours, or shows pornography against a woman's will, or make sexually coloured remarks shall be punished for the offence of sexual harassment which includes rigorous imprisonment for a term of three years, or with fine, or both.
- **Section 354B:** This section speaks about **assault or use of criminal force to women with intent to disrobe**. It says that any person who assaults or uses criminal force against a woman with the intent to disrobe her or compel her to become naked shall be punishable with imprisonment for a term of no less than three years, which may extend up to seven years, along with a fine.
- **Section 354C:** This section speaks about **'voyeurism'** which states if any person engages in any private act or captures the image of a woman shall be punished with an imprisonment for one year which may extend up to three years in first conviction and in case of second conviction the imprisonment shall be for three years which may extend up to seven years.
- **Section 354D:** This section speaks about **'stalking'** which says that any man who continues to follows a woman even after a clear indication of disinterest by such woman shall be convicted for the offence of stalking. It prescribes a punishment of imprisonment which may extend to three years in case of first conviction and may extend to five years in case of second conviction.
- **Section 499:** This section deals with the offence of **'defamation'** which is a gender neutral clause. It states that anyone who makes or publishes statements, signs, or representations about a person with the intent or knowledge that it will harm their reputation is considered to have defamed that person.

- **Section 503:** This section deals with **'criminal intimidation'** which states that anyone who threatens harm to a person's reputation, property, or someone they care about, with the intent to cause fear or force them to act against their legal rights, commits criminal intimidation.

Though the IPC has been in force since a very long time, it has been replaced by the new legislation that is the **Bhartiya Nyaya Sanhita, 2023.** This legislation aimed at replacing the colonial justice system by reforming and modernizing the criminal justice system. The primary goal of the Bhartiya Nyaya Sanhita is to ensure more efficient, accessible and equitable justice while addressing the challenges of modern crime.[178] The introduction of this new criminal law has marked a watershed moment in the Indian legal history which aimed to create a citizen-centric legal structure which addressing the contemporary needs of the Indian population. Recognizing the growing impact of technology-driven offenses against women, the Bhartiya Nyaya Sanhita has effectively addressed this issue through various provisions. However, despite the amendments made regarding the punishment for cybercrimes against women, no significant changes have been observed in the provisions themselves. The following table presents a comparison between the IPC and the BNS:-[179]

Subject	**IPC Section**	**BNS Section**	**Comparative Analysis**
Assault or use of criminal force to woman with intent to outrage her modesty.	Section 354	Section 74	No Change
Sexual harassment	Section 354A	Section 75	No Change
Assault or use of criminal force to woman with intent disrobes.	Section 354B	Section 76	The word 'any man' in the first has been replaced by 'whoever'
Voyeurism	Section 354C	Section 77	No Change
Stalking	Section	Section 78	No Change

[178] Renjith Thomas, *'Bhartiya Nyaya Sanhita,2023 : A Critical Perspective'* (2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4898463> accessed 11th February, 2025

[179] NCRB, *'Comparison summary of BNS and IPC'* (2024), <https://bprd.nic.in/uploads/pdf/COMPARISON%20SUMMARY%20BNS%20to%20IPC%20.pdf> > accessed 11th February, 2025

	354D		
Sale, etc., of obscene books, etc.	Section 292	Section 294	The term 'including display of any content in electronic form shall be deemed to be obscene' is inserted The fine is increased from two thousand to five thousand in first conviction and from five thousand to ten thousand in second conviction
Defamation	Section 499	Section 356(1)	The section is included as a sub-section
Defamation punishment	----	Section 356(2)	The section is included as a sub-section "or with community service" is added as a punishment
Criminal Intimidation	Section 503	Section 351(1)	No change. The section is included as a sub-section
Criminal Intimidation punishment	----	Section 351(2)/(3)	No change. The section is included as a sub-section

Digital evidence has become a fundamental element in the contemporary legal system, profoundly transforming the way investigations, litigation, and judicial processes are carried out. The **Bhartiya Sakshya Adiniyam, 2023** therefore revised the Indian Evidence Act, 1872 for the incorporation of digital evidence, thereby highlighting the growing significance of technological advancements in legal proceedings. The new legislation has focused in the admissibility of digital evidence and also enhances the handling of electronic evidence in cases related to cybercrimes.[180] **Section 2(1)(e)** which defines the term **'evidence'** has included electronically given statements in the definition. Moreover, a new section i.e. **Section 61** is added in the act which states that the admissibility of digital or electronic record as evidence cannot be prevented solely on the basis that it is an electronic record and it shall carry the same legal effect, validity and enforceability as any other document. The section 65B of the Indian Evidence Act which talks about 'admissibility of electronic records' has

[180] Prithwish Ganguli, 'Admissibility of Digital Evidence under Bhartiya Sakshya Adhiniyam: A comparative study with the Indian Evidence Act' (2024) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4977238> accessed 11th February,2025

been repealed in **Section 63** and other electronic records such as 'semiconductor memory', 'communication devices' has also been added.[181]

The **Protection of Children from Sexual Offences Act, 2012**, also addresses crimes related to cybercrimes committed against women and children. While the act primarily targets offenses against children, it also includes girls under the age of 18 within the scope of cybercrimes against women. **Section 11** of the Act defines **'sexual harassment'** as an offense committed by a person with sexual intent who either utters or makes any sound, forces a child to display their body, or threatens to use any form of media—such as electronic, film, digital, or other modes—to create or circulate a real or fabricated image of any part of the child's body or involve the child in a sexual act. **Section 13** of the Act addresses the **"use of a child for pornographic purposes,"** stating that anyone who exploits a child for sexual gratification through any form of media, whether by depicting sexual organs or any indecent representation of a child, is committing an offense. The term "use a child" encompasses the involvement of a child through any medium, including print, electronic, or other technological means.[182] This Act also covers sexual offenses committed through electronic mediums, acknowledging the role of digital technologies in facilitating child exploitation.

Article 19 and Article 21 of the **Constitution of India, 1950** offer protection to women against cybercrimes. Article 19(1)(a) grants the fundamental right to freedom of speech and expression. However, this right is not absolute and is subject to reasonable restrictions outlined in Article 19(2). Additionally, Article 21 guarantees women in India the right to live in cyberspace with dignity and respect.[183]

The **Copyright Act, 1957** also provides protection to women, **Section 63B** of this act deals with the protection of women from Data Theft which states that any person who knowingly makes use of a computer or an infringing copy of a computer program shall be punishable with an imprisonment for seven days which can extend to three years and a fine of fifty thousand rupees which may extend to two lakh rupees.[184]

---

[181] NCRB, *'Comparison summary of BSA and IEA'* (2024), <https://bprd.nic.in/uploads/pdf/Comparison%20Summary%20BSA%20to%20IEA.pdf > accessed 11th February, 2025

[182] Protection of Children from Sexual Offences Act 2012 (India)

[183] Constitution of India,1950

[184] Copyright Act, 1957(India)

5.2. Landmark Judgements

In any legal system that embraces a democratic form of government, the judiciary plays a crucial role. It is the most important branch of government, responsible for resolving conflicts between parties. For society's development, a smooth and effective adjudicative authority is essential. As society evolves, the role of the judiciary has become even more significant. In the age of information and technology, criminals are increasingly utilizing advanced technologies to commit crimes. Therefore, a proper judicial approach to addressing technological offenses is necessary for crime prevention. For the judiciary to function effectively, the rules of jurisdiction are vital. A key challenge in cases of cybercrime lies in issues related to jurisdiction.[185] In India, the judiciary is an independent body that plays a crucial role in interpreting and applying the law. However, challenges arise when offenses involve complex technical aspects that require specialized knowledge to determine whether an act constitutes a crime. This issue is particularly prevalent in cases of cybercrime, where the legal system faces numerous difficulties. While the laws themselves may be insufficient, the real challenge lies in the lack of technical expertise within the policy-making and operational systems. From a judicial perspective, a key issue is jurisdiction. Traditional laws, such as the Indian Penal Code and the Code of Criminal Procedure, provide provisions for territorial and extraterritorial jurisdiction. However, the unique nature of cybercrimes often demands more than what these conventional rules can offer, indicating a need for reform in the legal framework.[186] There has been various judicial pronouncements related to cybercrime against women where the court has focused in protecting women in the digital platforms.

1. **State of Tamil Nadu vs. Suhas Kutti**,[187] This was the first conviction under the Information Technology Act, 2000, marking a significant milestone in India's approach to cybercrime. The judgment, delivered in 2004, came just seven months after the FIR was filed, resulting in the conviction of the accused for cybercrime. The Honourable Additional Chief Metropolitan Magistrate passed the conviction order. In this case, the victim, a divorcee, was repeatedly harassed by annoying phone calls, with the perpetrator presuming she would respond positively due to a message she posted in a Yahoo message group, followed by forwarded emails. The message was obscene, defamatory, and disturbing. The accused turned

[185] Rajat Pahuja, *'Law Relating to Cyber Crime and Judiciary' (2023)* 4 IJRPR 3094
[186] Supra Note 3.
[187] State of Tamil Nadu vs. Suhas Kutti, CC No. 4680 of (2004)

out to be a family friend who was interested in marrying the victim. He was found guilty of offenses under Section 469 (forgery) and Section 509 (word, gesture, or act intended to insult the modesty of a woman) of the Indian Penal Code, as well as Section 67 (publishing obscene material in electronic form) of the Information Technology Act, 2000. The accused was convicted and sentenced to two years of rigorous imprisonment (RI) under Section 469 IPC, with a fine of Rs. 500. For the offense under Section 509 IPC, he was sentenced to one year of simple imprisonment and a fine of Rs. 500. For the offense under Section 67 of the IT Act, 2000, he was sentenced to two years of rigorous imprisonment and a fine of Rs. 4,000.[188]

2. **Manish Kathuria vs. Ritu Kohli**,[189] This was the first case of cyberstalking in India, involving Manish Kathuria, who stalked an Indian woman, Ms. Ritu Kohli, by impersonating her on the website www.mirc.com. He used her name, employed obscene and abusive language, and shared her home phone number, encouraging others to contact her. As a result, Ms. Ritu Kohli began receiving obscene calls from various states within India and abroad, with callers engaging in inappropriate conversations. Distressed by the situation, she contacted the Delhi police and reported the incident. The police registered the case under Section 509 of the Indian Penal Code, 1860, for outraging the modesty of a woman. However, Section 509 only addresses acts, gestures, or words intended to insult a woman's modesty, and does not account for such offenses when committed over the internet. This case raised alarms within the Indian government about the need to amend existing laws to address such crimes and better protect victims. In response, the Indian legislature amended the Information Technology Act, 2000, in 2008 to introduce provisions related to cyberstalking. While the IT Act, 2008 does not specifically mention stalking, it addresses the issue as an "intrusion into the privacy of an individual" rather than treating it as a conventional cybercrime. Consequently, the most commonly used provision to regulate cyberstalking in India is Section 72 of the IT Act, 2008.[190]

3. **State Cyber Cell vs. Yogesh Pandurang Prabhu**,[191] The present case involves the sending of obscene materials via email. Yogesh was accused of cyberstalking by sending

[188] Dr. Sapna Sukrut Deo, *'Cyberstalking and Online Harassment- A new challenge for law enforcement'* <http://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D9CA06D965AA9.pdf> accessed on 15th January, 2025

[189] Manish Kathuria vs. Ritu Kohli (2001)

[190] V.M. Eshwar,Aswathy Rajan, *'A Critical Analysis on Judicial Activism in Relation to Cyber Law-An Indian Perspective'* <https://acadpubl.eu/hub/2018-119-17/2/123.pdf> accessed on 15th January, 2025

[191] State Cyber Cell vs. Yogesh Pandurang Prabhu, CC No. 686/PS/2009

obscene emails to a female reporter. The court ruled that the accused had intentionally and knowingly violated the reporter's privacy, thereby violating Section 66E of the Information Technology Act, 2000, as well as Section 509 of the Indian Penal Code (IPC). However, the charges under Sections 67 and 67A of the Information Technology Act, 2000, were not proven beyond a reasonable doubt. As a result, the accused was convicted under Section 509 of the IPC and Section 66E of the Information Technology Act, in accordance with Section 248(2) of the Criminal Procedure Code (CrPC)[192]

4. **Avinash Bajaj vs. State (N.C.T) of Delhi**,[193] In this famous Bazee.com case, CEO Avinash Bajaj was arrested following an advertisement posted by a user offering to sell the DPS sex scandal video. Although the video was not uploaded on the platform, Avinash Bajaj was arrested under Section 67 of the Information Technology Act. This case led to the introduction of the Intermediary Guidelines in 2011, which stipulate that intermediaries can be absolved of liability if they exercise due diligence to prevent the display of obscene content on their platforms. The court granted bail to Mr. Bajaj, subject to him providing two sureties of Rs. 1 lakh each. Additionally, the court ordered Mr. Bajaj to surrender his passport and not leave India without prior permission. He was also instructed to cooperate with the investigation and assist as required. [194]

5**. State of Tamil Nadu v. Dr. L. Prakash**,[195] was a landmark case in which Dr. L. Prakash was sentenced to life imprisonment in connection with a case involving online obscenity. Dr. Prakash was a renowned medical practitioner and had contributed over 120 articles to reputed medical journals. He was convicted under Section 67 of the Information Technology Act This case was significant not only for the conviction but also because it highlighted the determination of law enforcement and the judiciary to hold accountable even highly educated and sophisticated professionals in India. However, a writ petition was filed requesting to grant him the privileges of a 'special class prisoner but the court dismissed the petition, denying him any special treatment.

[192] Priya Gupta, *'Cyber Stalking Against Women in the Indian Perspective: An Overview'* (2024) 29 IOSR-JHSS 58
[193] Avinash Bajaj vs. State (N.C.T) of Delhi (2004)
[194] Garima Tiwari (2014), Understanding Laws: Cyber Laws and Cyber Crimes, 1st Edition, 2014, p. 135
[195] State of Tamil Nadu v. Dr. L. Prakash, writ petition no. 7313 of 2002

6**. Tamal Chakraborty v. State of West Bengal,**[196] this case involved a woman who was stalked and harassed online by a man who shared her private images and personal information without consent. The accused was charged under various sections of the IPC, including Section 66C and Section 66E of the Information Technology Act, dealing with identity theft and violation of privacy.

6. **Fatima Riswana v. State Rep. by ACP., Chennai & Ors**,[197] In this case, both the public prosecutor and the counsel for the petitioners requested the court to transfer the case to another (male) judge in order to spare the district's female judge from the embarrassment of having to view certain CDs that were part of the evidence. The court agreed to the transfer, justifying the decision by stating that the trial would involve the exploitation of women and their use in sexual activities by the accused. Since the evidence in the case was in the form of CDs, which would need to be viewed during the trial, it was felt that it would cause undue embarrassment for a female presiding officer.[198]

7. **Aarti Tiwari v. State of Chandigarh**,[199] In this case, the accused were involved in the illegal recording of obscene videos and photographs of their patients at the clinic. The accused were tried under **Sections 66E, 67,** and **72** of the **Information Technology Act, 2000** for the unauthorized recording and transmission of personal and obscene material. Additionally, the accused were charged under **Section 509 of the Indian Penal Code (IPC)**, which pertains to the use of words, gestures, or acts intended to insult the modesty of a woman. Furthermore, they were tried under **Sections 4** and **6 of the Indecent Representation of Women (Prohibition) Act, 1986**, which prohibits the indecent representation of women through visual media.

8. **State v. Jawant Kumar Das**,[200] In this case, Jawant Kumar Das was arrested in 2012 for uploading defamatory remarks about a journalist's wife on an obscene website. He posted the offensive content as an act of revenge against her husband, who had exposed his illegal money lending business in the print media. The court found him guilty of posting the obscene material and convicted him on the charges brought against him

[196] Tamal Chakraborty v. State of West Bengal (2019)
[197] Fatima Riswana v. State Rep. by ACP., Chennai & Ors AIR 2005 712
[198] Nidhi Arya *"Cyber Crime Scenario in India and Judicial Response"* (2019) 4 IJTSRD 1108
[199] Aarti Tiwari v. State of Chandigarh, MANU/CG/0285/2014
[200] State v. Jawant Kumar Das, Manu /TN/0676/2002

9. **Shreya Singhal vs. Union of India,**[201] In this case, **Section 66A** of the **Information Technology Act, 2000** (inserted through an amendment in 2008) was declared unconstitutional by the Supreme Court. The court made this historic decision after a petition argued that the provision was overly vague and had been widely misused to suppress freedom of speech in cyberspace in India. While the provision was recognized as potentially draconian, the Supreme Court had an opportunity to reframe and amend the provision to regulate certain types of speech that could be categorized as 'harmful discourse' on the internet. It's important to note that issues like cyberbullying, trolling, online gender harassment, smishing, and vishing are becoming increasingly prevalent in India. The court could have considered the therapeutic jurisprudence value of **Section 66A** to create a more effective and balanced law to address these issues.[202]

10. **State vs. Ts. Balan and Aneesh Balan**, The Additional District Court and Sessions Court upheld the lower court's verdict in the first cybercrime case, State vs. T.S. Balan and Aneesh Balan, in which a Pentecostal Church priest and his son were sentenced to rigorous imprisonment in 2006. Disposing of the appeal filed by the priest, T.S. Balan, and his son, Aneesh Balan, against the Chief Judicial Magistrate's order, Additional District Judge T.U. Mathewkutty emphasized that it was time for the government to take effective measures to curb the growing trend of cybercrimes in the state. The court upheld the magistrate's decision, sentencing the two to three years of rigorous imprisonment and imposing a fine of Rs. 25,000 under Section 67 of the Information Technology Act. They were also awarded six months of rigorous imprisonment under Section 120(B) of the Indian Penal Code and one year of rigorous imprisonment with a fine of Rs. 10,000 under Section 469 of the IPC. The court, however, revoked the sentence under Section 66 of the IT Act. The cybercrime incident dated back to January-February 2002, with T.S. Balan and his son becoming the first individuals to be convicted for committing a cybercrime. They were found guilty of morphing and web-hosting nude pictures of Pastor Abraham and his family, which were then e-mailed from fake mail IDs with captions. Balan had worked with Pastor Abraham until they had a falling-out, after which he was expelled. He later joined the Sharon Pentecostal Church. The prosecution alleged that the accused had morphed photographs of Pastor Abraham, his son, Valsan Abraham, and his daughter, Starla Luke, and sent them via e-mail. The morphed pictures

[201] Shreya Singhal vs. Union of India, CC 167 of 2012

[202] Halder Debarati, A Retrospective Analysis of S.66a: Could S.66a of the Information Technology Act Be Reconsidered for Regulating 'Bad Talk' in the Internet? (August 1, 2015). Indian Student Law Review (ISLR), Vol. 3, pp. 91-118

were also posted online. The accused, who edited a local magazine called The Defender, had written about the photos in the publication. When Valsan Abraham received the pictures, he asked his father to file a police complaint. Following a police raid at the Balan household in Perumbavoor, evidence was collected. The magistrate's verdict came after a four-year trial, during which the court had to procure a computer with an internet connection and other necessary accessories. The police also enlisted the services of a computer analyst to piece together the evidence. In total, 29 witnesses, including representatives from the internet service provider and Bharat Sanchar Nigam Ltd., testified before the court.[203]

11. **Sreekanth C.Nair vs Licensee/Developer,**[204] A student from ASCL came across the website "www.incometaxpune.com" and, upon visiting the site, was redirected to a pornographic website. The complainant then approached the court seeking an order to block the website. The court ruled that such a request could only be made after the authorities listed under Clauses (i) to (vii) had either refused or shown no inclination to file a complaint with the Director of CERT-In. Only then could the court issue directions to the concerned officer. Another notable case is the DPS MMS scandal, which involved a compromising video clip of a schoolgirl being circulated on the internet. Additionally, there was the case of a Swiss couple in Mumbai who exploited slum children for pornography. The Mumbai police detained the couple for their involvement in this crime..[205]

12. **Kirti Vashisht v. State of Delhi,**[206] In this case, the petitioner, Kirti Vashisht, became a victim of revenge porn when her former lover shared intimate images and videos of her online without her consent. The accused was charged under **Sections 67** and **67A** of the **Information Technology Act, 2000**, which deal with penalties for publishing or distributing obscene or sexually explicit material online. The court ruled in favor of the victim, leading to severe punishment for the offender.

13. **Sree Surya v. State of Kerala,**[207] In this case, a college student filed a complaint after being repeatedly targeted by cyber-stalking and online abuse. The accused, who persistently sent threatening and abusive messages to the victim, was charged under **Section 354D** of the

[203] Shweta Krishnappa, *'Cyber-Bullying And The Related Laws In India' (2018)* <http://www.legaleraonline.com/articles/cyber-bullying-and-the-related-laws-in-india> accessed on 16th January, 2025
[204] Sreekanth C.Nair vs Licensee/Developer (2008)
[205] Supra Note 4.
[206] 2019 SCC Online Del 11713
[207] Sree Surya v. State of Kerala, Kerala High Court Case No. 2022

IPC (stalking) and **Section 66A** of the **Information Technology Act**. The court took a strong stance and convicted the accused.

14. **Kalindi Charan Lenka v. State of Odisha**:[208] In this case, the accused was charged with creating fake social media profiles of a woman and posting defamatory content about her, leading to harassment and emotional distress. The case was prosecuted under **Section 67** of the **Information Technology Act** and **Section 500** of the **IPC** (defamation). The court convicted the accused, highlighting the importance of safeguarding women from online identity theft and defamation.

15. **Neha Ghai case**,[209] in another case of cyber-stalking, a 20-year-old woman, Neha Ghai, was shocked to receive objectionable calls, messages on her mobile, and vulgar emails. She filed a police complaint against the accused for cyber-stalking, and the investigation proceeded by tracing the IP address of the system used by the accused to commit the offense.

16. **Salem case**, In this case, a 21-year-old woman took her own life after enduring severe online harassment. She had filed a police complaint against a man she suspected of creating and sharing obscene morphed images of her on Facebook. This suspicion arose after she had rejected his marriage proposal, and he allegedly acted out of spite and revenge. Following her initial complaint, further distress was inflicted upon her when another manipulated image was posted, this time tagged to her Facebook profile along with her name and her father's phone number. In her suicide note, the young woman repeatedly asserted that she had never sent such pictures to anyone. This heart-breaking case highlights the immense pressure and social stigma faced by victims of cybercrime, which can tragically lead to such extreme measures instead of fostering an environment of support and justice.[210]

17. **Kamlesh Vaswani v. Union of India**,[211] In this case, Mr. Vaswani filed a petition before the Supreme Court of India, challenging Sections 66, 67, 69, 71, 72, 75, 79, 80, and 85 of the Information Technology Act, 2000, and requesting a ban on all online pornography. He also sought for the consumption and dissemination of pornography to be classified as a non-baillable and cognizable offense. During the proceedings, the Department of Telecommunications instructed ISPs to block over 800 websites allegedly hosting

[208] Crl. Appeal No. 157 of 2018
[209] Dr. Karnika Seth, 'Cyber Crimes Against Women' (2018)
[210] Ibid.
[211] Kamlesh Vaswani v. Union of India (2016)

pornographic content, despite concerns about freedom of expression and privacy raised before the Supreme Court.

18. **Sabu Mathew George vs. Union of India,**[212] This is a 2008 case in which a writ petition was filed to ban advertisements related to pre-natal sex determination from search engines in India. Several orders have been issued, and the state has now established a nodal agency responsible for providing search engines with a list of websites to block. A key issue in this case is the "doctrine of auto-block." In one of the orders, the Court listed approximately 40 search terms and directed that any attempt to search for these terms should be automatically blocked. This raises concerns about intermediary liability and the potential impact on free speech.

19. **Prajwala vs. Union of India,**[213] This is a 2015 case in which an NGO called Prajwala sent a letter to the Supreme Court expressing concerns about the distribution of videos depicting sexual violence on the internet. The letter highlighted the widespread circulation of such videos on online platforms. In response to the letter, the Court registered a suo motu petition. Major tech companies, including Google, Facebook, WhatsApp, Yahoo, and Microsoft, were also included as parties. A committee was formed to "assist and advise the Court on the feasibility of preventing the circulation of videos depicting rape, gang rape, and child pornography."

20. **MMS case – of an Adibasi girl in Birbhum,** In this case, a 16-year-old Adivasi girl in 2010, working as a daily wage labourer, faced severe punishment by the local Panchayat for her relationship with a non-tribal boy from a neighbouring village. As a cruel and humiliating consequence, she was publicly stripped, forced to walk through the village, sexually harassed, and photographed by the villagers, with these images then being circulated within the community. Initially, no police case was registered against her attackers, and reports indicated that community leaders were the very individuals responsible for these criminal acts. However, the girl bravely filed a police complaint against six primary accused individuals, leading to their arrest. For her safety and well-being, she was placed in a government welfare home and is currently pursuing her education.[214]

[212] Sabu Mathew v. Union of India.(2008)
[213] Prajwala v. Union of India(2015)
[214] UNICEF, "Child Online Protection in India Report, 2016

5.3. Challenges in Addressing Cyber Crime Against Women

Cyber-crimes against women in India are a growing concern, and efforts to address them are complicated by a number of challenges. In this section, we will explore some of the key challenges that law enforcement agencies and the legal system face in addressing cyber-crimes against women in India.[215]

1. **Lack of Resources:** One of the main challenges is the lack of resources available to law enforcement agencies to investigate and prosecute cyber-crimes. Cyber-crimes are often complex and require specialized knowledge and technology to investigate. However, many police departments in India are understaffed and lack the necessary resources to handle cyber-crime cases effectively. This can result in delayed or inadequate investigations and low conviction rates.[216]
2. **Low Reporting rate of Cyber-crimes against Women:** Another challenge is the low reporting rate of cyber-crimes against women. Many women may not report incidents of cyber-crimes due to fear of retaliation or social stigma, or because they are not aware of their rights or the available legal remedies. This underreporting can make it difficult for law enforcement agencies to accurately assess the prevalence of cyber-crimes against women and allocate resources accordingly.[217]
3. **Digital Evidentiary Challenges:** The main challenge is in computer crime mostly all evidence in digital form. It has been very complicated for investigators to find, preserve digital evidence and also difficult for judges and lawyer to address court. S.65 (B) of the Indian Evidence Act is also create problems in the case of Foreign Service provider sharing evidence. As foreign company generally do not provide certificate, due to that Court has to reject evidence so Indian legislature has to take cognizance and has to made necessary amendment in the said section as per necessities of the digital era.[218]
4. **Traditional way of investigation:** which is failed in cybercrime. Due to increasing use of ICT, need the new investigations instruments. So for that special technological

[215] Canadian Centre for Cyber Security. (2021). Cyber threats to Canadian individuals and organizations. https://cyber.gc.ca/en/guidance/cyber-threats-canadian-individuals-and-organizations.
[216] Mr. Harish Yadav, '*Unveiling the Dark Side of Cyberspace: A Study of Cybercrimes against Women'* (2012) 11 IJFANS 3408
[217] Misra, Rajat, *'Cyber Crime against Women'* (2013). <https://ssrn.com/abstract=2486125 or http://dx.doi.org/10.2139/ssrn.2486125> accessed on 15th January 2025 at 04:03pm
[218] Supra Note 10

knowledge and skill should be required in investigation, prosecution and conducting cybercrime trial.

5. **Jurisdiction:** To decide Jurisdiction is also main challenging point for judiciary while deal the cyber offences. Cybercrime basically borderless crimes. In such kind of specific crime to decide jurisdiction is very complicated issue for the criminal justice system. United nation has also identified jurisdiction in cybercrime as major challenge. Even Indian government has also acknowledged that to decide jurisdiction in cyber offences as major challenge for Judiciary. In this kind of matter Supreme Court has directed to the government to create common portal for reporting cybercrime.
6. **No specific Legal Provision:** for the protection of individual rights at cyberspace. IT Act 2000 give general protection to the women victim at cyberspace. In 2008 Indian law makers has amended IT Act 2000 but still new form of cybercrime still not covered. Which also create problems in cyber trial for judiciary. Criminal justice has taken cognizance in while drafting national policy and directed the Indian legislature to reclassification of the existed cyber code.[219]
7. **Operational challenges:** As per the Sec.78 of the IT Act 2000 only inspector rank police officer do investigation in cyber offences. This section has created major challenge at practical level and indirectly affecting in judicial process. Which increasing pendency of court cases and create hurdles in speedy trials. Apart from that non-cooperation from service provider is also major challenge as state has not had control over the Internet.
8. **Paucity of technical tools and skilled human resources:** Judiciary face the root cause problem due to lack of technical tools, shortage of technical skilled manpower and infrastructure which increase hurdles in court proceedings. In 2017 Indian parliament has also rectified the problem of training of human resources who deal with cybercrime and also suggested nodal agency for cybercrime.[220]
9. **Gap between Technology and Knowledge:** There is gap between developing technology and traditional knowledge for new emerged cybercrime with the traditional criminal justice system. There are no settled legal procedure standards for dealing new form of cyber offences and no legal specific provisions for specific

[219] Himani Ahlawat, 'Cyber Crimes Against Women' (2024) 5 JVPA 1539
[220] Ibid.

crime. So during cyber trial judges faced lots of problems in trial and to deliver the judgment.

In India Judiciary is playing crucial role in the protection and safety and right of the women at cyberspace. Indian Judiciary has been trying to fill up the loopholes of Information Technology Act 2000. In so many cases judiciary has protected the right of women at cyberspace. But in changing scenario various kind of new developments at cyberspace lead to different kinds of cybercrimes and which are unnoticed. So in India needed such cyber savvy judges who can easily handle and fairly justified cybercrimes. Apart from that social awareness and advancement regarding individual's cyber rights is very poor, which need of the time to create awareness among society. So all the Constitutional machinery has to try their level best for the social awareness regarding cybercrimes and to take measurements to curbing the cyber issues and cybercrimes.

CHAPTER:- 6

CONCLUSION

Crime in any form has a detrimental impact on all members of society. In the present scenario, the prevalence of cybercrime has seen a rapid growth as it is driven by the widespread Internet usage and the digitalisation of economic activities. The rising trend of cybercrimes has raised an alarming issue not only in India but globally, financial crimes, harassment crimes and various other online crimes have posed threat on the society. As technology is rapidly rising, it has deeply penetrated nearly in every aspect of life starting from corporate governance to small-scale shopkeepers. Computers and electronic devices have become so integral to our daily life that it is now nearly impossible to imagine a day without the use of a computer or mobile phone. Today, the cyber space has been a blessing to someone and a curse to others. Irrespective of the gender, every person is prone to some form of cyber harassment or crimes. However, online harassment, victimization and other subsequent damages harms women more than men. Women have long been subjected to various forms of discrimination and crime, with cybercrimes emerging as a new and growing threat. Studies indicate that computer literacy rates are generally higher among men than women, which contributes to the increased vulnerability of women to cybercrimes.

Regardless of the amount of time they spend online, women are at risk of experiencing cyber violence. As previously discussed, a significant number of cybercrime cases in India go unreported. Victim-blaming remains a major deterrent, compelling many women to remain silent about the offenses committed against them. Rather than reporting abusive, threatening, or sexually explicit messages, most women and girls choose to block or ignore the perpetrators. It has also been observed that traditional crimes committed in physical spaces—such as rape, sexual molestation, blackmail, and stalking—have taken on new dimensions with the advancement of information and communication technology. Instances have emerged where perpetrators record acts of sexual violence, including rape, on mobile devices, and then use these images to extort money by threatening to make them public. There are also cases involving the grooming of women for exploitation in online pornography markets. Additionally, incidents have been reported where adolescent female students are sexually exploited by teachers who expose them to sexually explicit content through mobile phones or computers.

It has been found that over the five years i.e.2018-2022 there has been a significant rise in cybercrimes against women. Crimes such as fake profile, defamation, stalking, pornography and blackmailing are the rising types of crimes that are seen against women. It has been seen that various cases goes unreported as women does not tend to report these types of crimes yet, the police and the other stakeholders plays an important role in controlling such crimes. In the present scenario, young girls and women are found to be the most vulnerable one's in the cyber space. Though there has been a rising trend of cyber-crimes against women, the digital forensics and the other stakeholders plays an important role in controlling such crimes. The branch of cyber-forensics has gained recognition after the advancement of technology in the criminal justice system. Today, numerous crimes are performed with the help of technological devices, crimes such as rape, sexual exploitation and other heinous crimes against women leaves a digital footprint. Women are often subjected to various forms of sexual exploitation, and the digital space is no exception. Many become victims of online abuse, including blackmail by perpetrators who gain access to their intimate photographs. Pornographic images and videos are often used to exploit them, and out of the perpetrators, majority of them were seen to be known to the victim. It has been observed that the online crime rates against women has been a hike and exploiting women sexually has been a major concern which has been much easier due to the anonymity of the technology. It has been

observed that often the perpetrator is known to the victim; either it's her ex-partner, neighbour or any person from the family.

The branch of cyber- forensics which is also known as digital forensics plays an important role in controlling cyber-crime against women. The cyber-forensics not only plays an important role in controlling cyber-crimes but also plays a huge role in preparing evidences and presenting it in court with a proper chain of custody. The investigation process includes the identification, collection, demonstration and documentation of the data to maintain a proper chain of evidence. It plays a huge role in determining the source of evidence and also to recover the damage associated with it. This branch is not only limited to cyber-crimes but is much wider as it helps in determining digital footprints of various crimes such as terrorism, rape and many more. As there has been a rapid advancement of technology, though the crime happens to be in the physical form, yet the perpetrators are seen to leave a digital footprint in order to stalk, harass or blackmail the victim. This branch of forensics deals with various other branches such as network forensics, cloud forensics, mobile forensics and many more. The digital evidences serves as a paramount in cases related to cybercrime against women and therefore following a proper chain of custody is really required. Today, the new laws though gives much importance to electronic evidence, yet it's admissibility in court depends on following a proper chain of custody. In cases related to cyber-crimes against women, it has been seen that branches such as network forensics, mobile forensics, computer forensics and social media forensics are used in these cases and evidences such as social media accounts, phone calls, whatsapp messages shows up in cases related to cyber-crime against women. Not all crimes are presented in court as it has been seen that there are certain crime such as cyber obscenity where obscene content takedown plays an important role in preventing such content from getting viral. In the UK, USA and Canada it has been seen that they have proper legal frameworks to control cyber crimes against women.

The Indian Judiciary plays an important role in controlling cyber-crimes against women. The apex court has given various judgements to control such crimes and many perpetrators have been convicted to control these crimes. The legal frameworks have also played an important role in controlling these crimes. The new criminal laws have given much importance to digital evidences and have mandated the requirement for forensic investigation of crimes that have more than seven years of punishment. Although the criminal justice system's stakeholders contribute significantly to combating crimes against women, the anonymity of the internet and several other factors still allow women to be targeted and victimized online.

BIBLIOGRAPHY

Statutes and Bills

1. Indian Penal Code, 1860
2. Code of Criminal Procedure, 1973
3. Indian Evidence Act, 1872
4. Bhartiya Nyaya Sanhita, 2023
5. Bhartiya Shakshya Adhiniyam, 2023
6. Information Technology Act, 2000
7. Protection of Children from Sexual Offences Act, 2012,
8. The Constitution of India, 1950
9. The Copyright Act, 1957
10. The UK Police and Criminal Evidence Act, 1984
11. Personal Information Protection and Electronic Documents Act, 2000
12. The Online Safety Act, 2023
13. The Data Protection Act, 2018
14. The Criminal Justice and Courts Act, 2015
15. The Protection of Harassment Act, 1997
16. The Malicious Communications Act, 1988.
17. The Violence Against Women Act,1994

Books

1. Cyber Crimes against Women in India, by Dr. Debarati Halder and K. Jaishankar, Sage publications, 2016
2. Cybercrime and the Victimization of Women: Laws Rights and Regulations, by Dr. Debarati Halder and K. Jaishankar, Sage publications, 2011
3. Cyber Forensics, by Mr. Dejey Murugan, Oxford Publication, 2018
4. Cyber Crimes Against Women: An Indian Law Perspective' by Dr. Karnika Seth, Oxford Publication, 2018
5. Cyber crime against women in India' by Dr. Sashya Mishra, Notion Press, 2023
6. Digital Forensics and Investigation Methods' by Dr. Padmavathi Ganapathi and Dr. Digvijay Singh, Notion Press, 2022

Dissertation edit 4.docx

My Files

My Files

Bennett University

Document Details

Submission ID
trn:oid:::3618:91738443

Submission Date
Apr 17, 2025, 9:40 PM UTC

Download Date
Apr 17, 2025, 9:42 PM UTC

File Name
Dissertation%20edit%204.docx

File Size
492.8 KB

88 Pages

26,954 Words

148,565 Characters

6% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Abstract

Match Groups

- 96 Not Cited or Quoted 6%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
1% Publications
3% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 96 Not Cited or Quoted 6%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
1% Publications
3% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet www.gapinterdisciplinarities.org	2%
2	Internet www.ijfans.org	<1%
3	Internet ccgnludelhi.wordpress.com	<1%
4	Publication Himani Ahlawat, Somlata Sharma. "CYBER CRIMES AGAINST WOMEN IN INDIA", S...	<1%
5	Internet www.sethassociates.com	<1%
6	Internet wilmap.law.stanford.edu	<1%
7	Submitted works Osmania University, Hyderabad on 2024-09-08	<1%
8	Submitted works National Law University, Jodhpur on 2025-04-15	<1%
9	Submitted works Savitribai Phule Pune University on 2019-04-24	<1%
10	Submitted works University of East London on 2025-01-07	<1%

11	Internet legallyin.com	<1%
12	Submitted works hpnlushimla on 2024-01-05	<1%
13	Submitted works The WB National University of Juridical Sciences on 2024-11-06	<1%
14	Internet ijaps.usm.my	<1%
15	Internet www.aaptaxlaw.com	<1%
16	Internet nualslawjournal.com	<1%
17	Publication "The Palgrave Handbook of International Cybercrime and Cyberdeviance", Spring...	<1%
18	Submitted works Uttaranchal University, Dehradun on 2023-07-05	<1%
19	Internet ijless.kypublications.com	<1%
20	Internet www.lawyersclubindia.com	<1%
21	Submitted works United Colleges Group on 2025-04-06	<1%
22	Submitted works University of Wollongong on 2023-12-13	<1%
23	Submitted works Aston University on 2025-01-08	<1%
24	Submitted works City University on 2021-10-18	<1%

25	Submitted works ESoft Metro Campus, Sri Lanka on 2025-04-04	<1%
26	Submitted works Sharda University on 2024-04-19	<1%
27	Submitted works Symbiosis International University on 2020-04-07	<1%
28	Submitted works University of Glamorgan on 2023-12-13	<1%
29	Submitted works University of Western Sydney on 2018-11-03	<1%
30	Internet core.ac.uk	<1%
31	Internet elar.naiau.kiev.ua	<1%
32	Internet legalserviceindia.com	<1%
33	Internet www.bahria.edu.pk	<1%
34	Submitted works King's Own Institute on 2019-09-26	<1%
35	Submitted works Maharishi University Of Information Technology, Lucknow on 2024-04-10	<1%
36	Publication Muhammad Zareen, Baber Aslam, Shahzaib Tahir, Imran Rasheed, Fawad Khan. "...	<1%
37	Submitted works NALSAR University of Law Hyderabad on 2013-11-09	<1%
38	Submitted works National Law School of India University, Bangalore on 2013-09-13	<1%

39	Submitted works Panjab University on 2025-02-17	<1%
40	Submitted works Tata Institute of Social Sciences on 2022-11-02	<1%
41	Submitted works National Law University New Delhi on 2017-04-27	<1%
42	Submitted works Rajiv Gandhi National University of Law on 2015-04-17	<1%
43	Submitted works The WB National University of Juridical Sciences on 2022-03-27	<1%
44	Submitted works Uttaranchal University, Dehradun on 2022-07-02	<1%
45	Submitted works Uttaranchal University, Dehradun on 2023-06-28	<1%
46	Submitted works Kingston University on 2019-09-24	<1%
47	Submitted works Rajiv Gandhi National University of Law on 2020-06-30	<1%
48	Submitted works Uttaranchal University, Dehradun on 2020-06-09	<1%
49	Internet babe.hr	<1%
50	Internet blog.ipleaders.in	<1%
51	Publication Balsing Rajput, Dhrumi Gada, Amit K. "Online Child Sexual Abuse", Springer Scien...	<1%
52	Internet academicworks.cuny.edu	<1%

53	Internet journals.iium.edu.my	<1%